



UNIVERSIDAD DE CHILE

Facultad de Derecho

Departamento de Estudios en Derecho Informático

**EL DERECHO A SER INFORMADO COMO SUSTENTO FUNDAMENTAL DEL
CONTROL DE DATOS PERSONALES**

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

PAULINA ALEJANDRA MOYA JIMÉNEZ

PROFESOR GUÍA: LORENA DONOSO ABARCA

Santiago, Chile

2010

DEDICATORIA

A mis padres.

AGRADECIMIENTOS

A la profesora Lorena Donoso Abarca, Doctora en Derecho y Magíster Universitario en Informática y Derecho por la Universidad Complutense de Madrid, Diplomada en Educación a Distancia por la Université du Québec y Licenciada en Ciencias Jurídicas y Sociales por la Universidad de Chile, por haber sugerido el tema, por sus ideas y apoyo en la elaboración de esta memoria.

Al profesor Francisco González Hoch, Magíster en Derecho, Universidad de Harvard, Doctorado en Derecho, Universidad de Chile, por su tiempo y dedicación en la revisión de esta memoria.

TABLA DE CONTENIDO

INTRODUCCIÓN	12
CAPÍTULO I	19
ANTECEDENTES HISTÓRICOS DE LA PROTECCIÓN DE DATOS EN DERECHO COMPARADO Y CHILE.	19
1.1. Antecedentes históricos que dan origen al tratamiento de datos personales y su regulación por el derecho.	19
1.2. Procesamiento de datos y tratamiento de datos personales.	25
1.3. Potencialidad dañosa que arraigan los registros de datos personales	34
1.3.1. Mega-archivos	34
1.3.2. Data Warehouse	35
1.3.3. Datavigilancia	38
1.4. Aproximación a los derechos fundamentales vulnerados en el proceso de tratamiento de datos personales y supuesta contraposición con los principios de necesidad de información, libre circulación de la información y derecho de información	43
CAPÍTULO II	50
CONFIGURACIÓN DEL DERECHO A CONTROLAR LOS DATOS PERSONALES Y HERRAMIENTAS PARA LA PROTECCIÓN DE LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES EN EL DERECHO COMPARADO Y CHILE.	50

2.1. Las primeras manifestaciones de vulneración de derechos por tratamiento de datos personales y como se concibió que se articulaban en torno a las concepciones de intimidad y <i>privacy</i> .	50
2.2. Mutación de la concepción de intimidad y <i>privacy</i> hacia el reconocimiento de un nuevo derecho llamado autodeterminación informativa y libertad informática.	57
2.3. Aceptación de la autodeterminación informativa y la libertad informática como derechos de control de datos personales.	63
2.4. Herramientas para la protección de los derechos de los titulares de los datos personales: el derecho a ser informado en sus distintas modalidades.	68
2.5. El derecho a ser informado en los primeros cuerpos normativos rectores	75
2.5.1. Convenio 108	76
i. El derecho a ser informado manifestado como derecho a conocer.	77
ii. El derecho a ser informado manifestado en el derecho a obtener a intervalos razones y sin demora o gastos excesivos la siguiente información.	77
iii. El derecho a ser informado manifestado en el derecho a obtener cuando corresponda la rectificación o borrado de los datos personales.	78
iv. El derecho a ser informado manifestado en la disposición de un recurso si no se ha atendido a la petición de confirmación, de comunicación, de rectificación y borrado.	78
2.5.2. Directiva 95/46/CE	79
i. El derecho a ser informado en caso de obtención de datos recabados del propio interesado.	79
ii. El derecho a ser informado en caso de obtención de datos que no han sido recabados del propio interesado.	80
iii. El derecho a ser informado manifestado como derecho de acceso.	81
iv. El derecho a ser informado manifestado como derecho de consulta ante la autoridad de control.	82
v. El derecho de información manifestado como derecho de rectificación, supresión o bloqueo.	84

CAPÍTULO III	86
CONFIGURACIÓN DEL CONTROL DE DATOS PERSONALES Y DEL DERECHO A SER INFORMADO EN LA LEGISLACIÓN COMPARADA Y EN CHILE	86
3.1. LEGISLACIÓN COMPARADA.	86
3.1.1. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución española y en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.	89
1. Derecho a ser informado en toda solicitud de datos personales.	93
2. Derecho a ser informado cuando los datos personales se recaben de terceros.	94
3. Derecho a ser informado manifestado como derecho de consulta al Registro General de Protección de Datos.	95
4. Derecho a ser informado manifestado como derecho de acceso.	96
5. Derecho a ser informado manifestado como derecho de rectificación y cancelación.	99
6. Derecho a ser informado en la prestación de servicios de información sobre solvencia patrimonial.	101
7. Derecho a ser informado en los tratamientos de datos con fines de publicidad y de prospección comercial.	101
Limitaciones al derecho a ser informado en sus distintas manifestaciones.	102
Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.	103
Jurisprudencia de la Agencia Española de Protección de Datos Personales y de la Agencia de Protección de Datos de la Comunidad de Madrid.	109
3.1.2. Los derechos del titular a controlar sus datos	120

personales y a ser informado en la Constitución argentina y en la Ley N°25.326 sobre Protección de Datos Personales.	
1. Derecho a ser informado al recabar datos personales.	125
2. El derecho a ser informado manifestado como derecho de acceso.	127
3. Derecho a ser informado manifestado como facultad de solicitar información al organismo de control.	130
4. Derecho a ser informado manifestado como derecho de rectificación, actualización, integración, bloqueo o supresión.	131
Limitaciones al derecho a ser informado en sus distintas manifestaciones.	133
Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.	134
3.1.3. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución colombiana y en la Ley Estatutaria 1.266.	141
1. Derecho a ser informado en el tratamiento general de datos personales.	145
i. Derecho a ser informado por la fuente de información.	145
ii. Derecho a ser informado por los operadores de los bancos de datos.	146
iii. Derecho a ser informado por los usuarios.	147
2. Derecho a ser informado en el tratamiento de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.	147
Incumplimiento de la obligación de informar al titular de los datos personales en sus distintas modalidades.	151
3.1.4. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución mexicana y en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.	155
1. Derecho a ser informado al recabar datos personales del individuo.	157
2. Derecho a ser informado manifestado como derecho de acceso.	158
3. Derecho a ser informado manifestado como derecho de consulta al listado de los sistemas de	159

datos personales.	
4. Derecho a ser informado manifestado como derecho de modificación.	159
Incumplimiento del deber de información en sus diferentes manifestaciones.	160
3.2. LEGISLACIÓN CHILENA.	161
3.2.1. La protección constitucional chilena frente al tratamiento de datos personales.	161
• Artículo 19 N°4	162
• Artículo 19 N°12	165
• Artículo 19 N°21	166
3.2.2. La Ley N°19.628 sobre Protección a la Vida Privada. El bien jurídico tutelado, sus principios formadores y los derechos del titular de los datos.	167
1. Sobre los titulares	169
2. Sobre los obligados	169
3. Sobre las obligaciones del titular del fichero	170
a) Obligación de informar	170
b) Obligación de confidencialidad y secreto	171
c) Obligación de seguridad en el tratamiento	172
d) Obligación de mantener registrados datos de calidad	172
4. Control del tratamiento de datos personales	174
a) Órgano fiscalizador	174
b) Responsabilidad por infracciones	175
c) Acción de reclamación y acción indemnizatoria	175
3.2.3. Desarrollo del derecho de información del titular de los datos personales y la efectividad de las tutelas ofrecidas en la ley.	176
1. Derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública.	176
2. Derecho a ser informado para autorizar el	178

tratamiento de datos personales	
3. Derecho a ser informado manifestado como derecho de acceso.	185
4. Derecho a ser informado manifestado como derecho de consulta frente al Servicio de Registro Civil.	187
5. Derecho a ser informado manifestado como derecho de modificación, eliminación y bloqueo.	188
Limitaciones al derecho a ser informado.	189
Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.	190
CAPÍTULO IV	195
LAS MODIFICACIONES LEGALES EN CHILE Y SU ADECUACIÓN AL ESTÁNDAR INTERNACIONAL DE PROTECCIÓN DE DATOS EN MATERIA DE INFORMACIÓN AL AFECTADO POR EL TRATAMIENTO DE DATOS PERSONALES.	195
4.1. Proyecto de Ley que introduce modificaciones a la Ley N° 19.628 sobre Protección a la Vida Privada y a la Ley N° 20.282 de Transparencia de la Función Pública y de Acceso a la Información Privada.	195
1. Derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública.	199
2. Derecho a ser informado en toda solicitud de datos al propio titular.	200
3. Derecho a ser informado en la recogida de datos desde terceros.	201
4. Derecho a ser informado para autorizar y realizar el tratamiento de datos personales.	202
5. Derecho a ser informado manifestado como derecho de acceso.	204
6. Derecho a ser informado manifestado como derecho de consulta frente al Registro Único Nacional de Bancos de Datos.	205
7. Derecho a ser informado manifestado como	206

derecho de modificación, eliminación y bloqueo.	
Limitaciones al derecho a ser informado en sus distintas modalidades.	207
Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.	207
4.2. Proyecto de Ley sobre deuda positiva y negativa de los chilenos.	211
1. Derecho a que se registre, comunique y difundan datos personales fidedignos, veraces y actualizados.	221
2. Derecho a ser informado por los aportantes a solicitud escrita del titular de los datos.	221
3. Derecho a ser informado manifestado como derecho de acceso.	226
4. Derecho a ser informado manifestado como derecho de rectificación y cancelación.	229
Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.	230
CONCLUSIONES FINALES	236
BIBLIOGRAFÍA	262

RESUMEN

En una de sus manifestaciones, la sociedad de la información permite a los individuos figurar en los medios de forma incógnita, sin necesidad de identificación, inmersos en el anonimato. No obstante, de forma simultánea, la tecnología, el tratamiento de la información circulante y su difusión en los medios, acarrea la apertura de la vida privada de las personas a través de la exposición de numerosa información personal.

Hoy en día, la información es vital para tomar decisiones informadas, valorándose por los actores del mercado como un bien susceptible de evaluación pecuniaria que mientras sea transado en mayores cantidades tiene posibilidades de ser más exacto, íntegro y consecuentemente útil. Las legislaciones de todo el orbe han venido planteando desde hace algunas décadas el derecho a la información como un derecho fundamental, estableciendo que el acceso a la información es una instancia necesaria de participación de la ciudadanía, que debe precisamente cautelarse a través de un definido derecho que posibilite la circulación de información adecuada, oportuna y veraz.

En este contexto ha surgido la protección de datos personales, cuya finalidad se centra en la estructuración de las condiciones sobre las cuales se permitirá hacer uso de los datos personales de las personas, estableciendo un conjunto de garantías contra la manipulación indebida por terceros de los datos personales, evitando que se vulneren diversos derechos fundamentales como la intimidad, la privacidad, la dignidad, el derecho a la salud, al trabajo, entre otros.

La noción del bien jurídico tutelado con la protección de datos personales ha debido avanzar hacia la conceptualización de un derecho de los titulares de la información a controlar los datos que le conciernen, el que se organizara en torno a las distintas manifestaciones del derecho a la información, posibilitándose que el individuo tome conocimiento acerca de que datos suyos están siendo tratados, ejerciendo las facultades de modificación, eliminación y bloqueo en caso que la información que conste en el banco de datos no se corresponda con la realidad.

Un sistema eficaz de protección de datos personales debe proveerse de instituciones sólidas que operen en caso de incumplimiento, de manera de desincentivar conductas fuera de la ley y promover la transparencia irrestricta de la información circulante.

INTRODUCCIÓN

La revolución científica y tecnológica puede ser observada por el ser humano desde distintos ángulos, dimensiones y perspectivas. Con el surgimiento y auge de los sistemas de computarización, el registro y la circulación de los datos personales crecieron inusitadamente, generándose lo que se denominó “el poder de la informática”, que detentan quienes poseen en sus manos información y pueden usarla para tomar decisiones más óptimas y acertadas.

El panorama de la humanidad cambió sustancialmente, planteándose la afirmación de que la tecnología, la informática y los computadores tienen que estar al servicio de los hombres y de las mujeres y, de ningún modo en la relación inversa. En efecto, reconocemos los beneficios que conlleva vivir inmersos en un mundo con crecimientos científicos ilimitados, pero advertimos la necesidad de proteger a las personas y la sociedad en su conjunto, a través de directrices claras que establezcan como debe ponderarse esta relación tecnología – ser humano.

En la actualidad, la cantidad de datos disponibles sobre una persona determinada, facilitados por los sistemas de mega-archivos, data warehouse y datavigilancia, pueden provocar para ella no solo una serie de beneficios -como facilidad de crédito comercial, celeridad en las transacciones, renombre profesional, ahorro de tiempo, eficacia, mayor información, capacidad de comunicación, comodidad, etc.- sino también una serie de inconvenientes de escalas no dimensionadas y que se materializan en la vulneración de derechos fundamentales del individuo, como lo son la libertad, la intimidad, el derecho a la salud, el derecho al trabajo, entre otros.

Esta potencialidad dañosa de los registros de datos personales ha sido parte de la moderna preocupación de juristas y legisladores de todo el mundo. Sin embargo, desde el punto de vista de las personas en su individualidad, no existe una real conciencia sobre el tratamiento del que está siendo objeto su información personal, pues al contrario de lo que sucede con las ventajas de la informática, que el hombre

disfruta a diario, los inconvenientes quedan relegados al silencio. Desde esta perspectiva, una de las premisas fundamentales sobre la que se asentará la protección de los datos personales dice relación con el desconocimiento de las personas sobre la cantidad efectiva de datos personales que están siendo recogidos en los bancos de datos de organismos públicos y privados y, la utilización que se les da a éstos.

Cuando frente al avance de la ciencia se encuentran los derechos de los individuos, nada debe ser dejado a la improvisación. El desafío para el derecho no consistirá en suprimir alguno de estos dos extremos, es decir, aceptar el sacrificio de los derechos en aras del avance tecnológico, ni a la inversa, anular el desarrollo de las tecnologías para promover una cautela íntegra a los derechos de los individuos. Precisamente el reto está en encontrar el punto de equilibrio que permita la convivencia pacífica de ambas partes, sin tener que lamentar consecuencias irreversibles para alguna de ellas.

Esta necesidad de equilibrio se agudiza aún más cuando el panorama internacional advierte el derecho a la información como un derecho fundamental, un pilar del Estado de derecho. El derecho a la información garantiza la libertad de pensamiento y permite el ejercicio del control ciudadano de la gestión pública, abarcando no sólo a los periodistas o empresarios de la información, sino a toda persona, y particularmente al Estado. Así, se ha considerado que si a las personas se les niega el acceso a la información, se les obstaculiza la expresión de sus pensamientos o se las priva de su derecho a emitir y conocer opiniones. De aquí que sea vital establecer cómo se jerarquizan y estructuran estos derechos en nuestro ordenamiento.

Analicemos el caso de nuestro país. Hoy en día, con solo poseer el Rol Único Nacional de una persona es posible obtener su nombre completo, fecha de nacimiento, dirección particular, estado civil, profesión, teléfono, identificación de sus padres, propiedades inmuebles y muebles que posee, prestaciones alimentarias sin pagar, historial judicial, solvencia económica y otros tantos datos. En Chile, a la mayoría de estos datos puede accederse desde terminales informáticas e imprimirlas en pocos segundos.

Sin menospreciar las múltiples posibilidades que otorgan estos sistemas y las nuevas herramientas disponibles, la temática podría adquirir contornos más delicados. Pensemos en la nueva red social que es *facebook*, millones de personas alrededor del mundo suscriben una cuenta en la cual van registrando una serie de datos personales que pueden ser de variada naturaleza y alcanzar los datos básicos ya mencionados, y sumando a éstos las preferencias personales, el lugar de trabajo, las actividades diarias, las personas conocidas, los amigos cercanos, la identificación de familiares y un sinnúmero de datos personales de diferentes características. ¿Cómo se regula esta gigantesca base de datos y cómo se utilizan éstos? Los usuarios lo desconocen y al leer la declaración de derechos y responsabilidades de la entidad no queda muy claro.

Otra controversia que comenzó a desarrollarse hace pocos meses es el sitio <http://trywho.bligoo.com/> que en su inicio se denominaba www.trywho.com. Al acceder a este sitio se puede obtener rápidamente el nombre de una persona, su RUT, su fecha de nacimiento, su estado civil, sus hijos, la ciudad de residencia, la empresa donde trabaja, la empresa en que trabajó o cualquier otra información vinculada a la persona que constara en fuentes de libre acceso al público, en la medida que se encontrara interconectada con los proveedores de este servicio. No obstante este servicio se ajusta a la ley, levantó el mayor revuelo causado por un servicio de esta naturaleza en Chile, principalmente porque mostró de manera descarnada las potencialidades del tratamiento de datos personales. En este caso, si bien la empresa no era un administrador de bases de datos, sino un simple nexo de comunicación entre fuentes de libre acceso al público y los usuarios que quieren utilizar la información, las operaciones que realiza pueden ser calificadas como de tratamiento de datos personales y por tanto el análisis debe realizarse a la luz de la ley del ramo.

Otro caso que salió a la luz pública fue el que dio a conocer el 27 de mayo de 2009 el senador Guido Girardi, quien anunció la presentación de querrelas criminales apoyando a Verónica Sánchez, una abogada que descubrió que su historial médico estaba en manos de una cadena de farmacias producto de una transferencia de datos desde su Isapre. Llamó mucho la atención este caso porque de acuerdo a la Ley N° 19.628 de Protección a la Vida Privada que regula el tratamiento de datos personales en Chile,

esta información es un dato personal de carácter sensible que se refiere a los estados de salud físicos o psíquicos de los individuos que no puede ser objeto de tratamiento, excepto cuando la ley expresamente lo autorice o el titular de los datos consienta en ello.

Precisamente estas alteraciones en la forma de vida de las personas son las que han obligado al derecho a delimitar jurídicamente los efectos de estos cambios mediante la regulación de postulados y también de consecuencias del tratamiento de datos personales, intentando crear un equilibrio entre los intereses en conflicto. El tema se vincula directamente, como decíamos antes, con los derechos fundamentales de las personas, con el respecto a su libertad, a su intimidad, a su dignidad y a una serie de derechos que pueden ser vulnerados tangencialmente.

Los derechos fundamentales no son absolutos y la recogida y manejo de datos sirve en una sociedad democrática para fines tan constitucionales como la generación de políticas sociales, económicas y culturales acordes a las necesidades de la sociedad. Entonces, el tema no puede ser objeto de premisas previas, debe aceptarse que el equilibrio es la única solución para la existencia de un efectivo derecho a la protección de datos personales que imponga un margen de orden y racionalidad en la esta relación del titular del banco de datos y el titular de la información.

La protección de datos personales, como consecuencia de su relativa juventud, no ha encontrado siempre una previsión constitucional o legal que la respalde. Por ello, en el momento que nace la necesidad de protegerse del avance progresivo del acopio de datos, surge también como prioritaria la necesidad de definir su naturaleza y contenido, vinculándola con otras categorías legales más consolidadas. A nivel internacional grandes han sido los avances que se han obtenido desde la suscripción del Convenio 108 y la Directiva 95/46 que fijan directrices claras, estableciendo un entramado de derechos y obligaciones de claro alcance para las partes de la relación. Estas mismas directrices se han acogido a nivel nacional en las diferentes legislaciones del mundo, las que a través de este marco han sido capaces de articular un verdadero régimen de protección de los datos personales con roles e instituciones operantes.

Tanto a nivel internacional como nacional hay consenso respecto a la existencia de acciones para tutelar los intereses del titular de los datos personales. La principal herramienta es la acción de hábeas data dispuesta para tomar conocimiento de los datos personales que constan en un registro y para solicitar su modificación, eliminación y bloqueo en caso que sea necesario, como presupuesto necesario para el reconocimiento del derecho a controlar los datos personales.

La presente memoria sostendrá que la protección de datos personales debe tener como punto de partida fundamental, para perfilar el contenido de su núcleo esencial, el principio de transparencia en el tratamiento de datos personales, el que se asentará sobre la base de que para que el titular pueda controlar la información que le concierne, debe proveérsele de un sólido derecho a ser informado, plasmado en distintas manifestaciones que dependerán de quién haya recogido los datos y del momento de acceso a éstos. El reconocimiento de este derecho como fundamento del control de los datos personales permitirá un equilibrio entre todos los actores inmersos en el tratamiento de datos personales, los intereses en pugna y el ejercicio de otros derechos del titular de los datos, que estarán relegados a la inexistencia de no proveérseles este derecho rector.

Para que el derecho a ser informado tenga una existencia óptima debe contar con instituciones efectivas, como un adecuado órgano de control y un sistema sancionatorio que desincentive las conductas ilegales por parte de los responsables de los bancos de datos. La existencia y operación eficaz de estas instituciones es un aspecto igualmente relevante que la consagración de derechos en sí misma, pues un derecho puede estar condenado a ser letra muerta si no se cuenta con una estructura adecuada que lo sostenga.

Para el cumplimiento del primer objetivo de esta memoria, es decir, para el establecimiento de una estructura base para la definición de un concepto de control de datos personales dotado de principios básicos y esenciales, en cuya base se encontrará el derecho de información del titular de los datos personales, avanzando

hacia la configuración de un concepto de transparencia informativa, esta memoria se estructurará de la siguiente forma:

En la primera parte, se otorgará al lector un marco general relativo al tratamiento de datos personales, otorgando una estructura conceptual sobre los términos que se asentará el derecho de protección de los datos personales. Se establecerán los antecedentes históricos de la materia, indagando en el desarrollo del procesamiento de datos y la potencialidad dañosa que arraigan los registros de datos personales. Se realizará una primera aproximación a los derechos fundamentales vulnerados en el proceso de tratamiento de datos.

En la segunda parte, se discurrirá íntegramente en el examen de la configuración del origen y desarrollo del derecho de protección y control de los datos personales y su relación con el derecho de información del titular de los datos, revelando como se ha avanzado desde las primeras manifestaciones de vulneración de derechos que se articulaban en torno a las nociones de intimidad y *privacy* hacia el reconocimiento de un nuevo derecho de control de los datos personales conceptualizado bajo los nombres de autodeterminación informativa y libertad informática, explicando cómo se vinculan éstos con el derecho a ser informado que asiste al titular de los datos. Además, examinaremos cuáles son las herramientas establecidas para la protección de los derechos de los titulares de datos personales en Derecho Comparado y Chile.

Luego, analizaremos el control de datos personales, el derecho a ser informado en la dimensión internacional y sus herramientas asociadas, a través de un estudio específico del caso de España, Argentina, Colombia y México, a través de sus Cartas Fundamentales y sus leyes de protección de los datos personales. Además, se analizará, en la dimensión nacional, la protección constitucional frente al tratamiento de datos personales y la Ley N° 19.628.

En la cuarta parte de este trabajo expondremos las modificaciones legales en Chile y su adecuación al estándar internacional de protección de datos en materia de información al afectado por el tratamiento de datos personales, a través del análisis de

los actuales proyectos de ley en el Congreso, sus principios formadores, los distintos derechos de información del titular de los datos y la efectividad de las tutelas ofrecidas en la ley.

Finalmente, concluiremos como se configura el concepto de control de datos personales en base a los derechos de información en sus distintas manifestaciones, fijando el contexto adecuado para una regulación eficaz a través de la identificación de falencias y fortalezas de los sistemas comparados y de nuestro sistema nacional.

CAPÍTULO I.
ANTECEDENTES HISTÓRICOS DE LA PROTECCIÓN DE DATOS EN DERECHO
COMPARADO Y CHILE.

1.1. Antecedentes históricos que dan origen al tratamiento de datos personales y su regulación por el derecho.

No hay duda alguna que hoy en día presenciamos una de las revoluciones más importantes que ha vivido el hombre, representada por las nuevas tecnologías de comunicación y la información, las que traen consigo una serie de transformaciones de índole económico, cultural, político y espiritual.

Algunos autores se aventuran a afirmar que esta revolución supera en magnitud, a la revolución industrial, pues el alcance que en nuestros días han cobrado las nuevas tecnologías superan con creces esta visión, no faltándole razón a los que piensan que más que ante una revolución histórica estamos en presencia de una nueva etapa de la humanidad¹.

Desde hace siglos, el papel es la memoria de la humanidad. Con la aparición de la imprenta a principios del siglo XV se manifestó la universalidad y la transmisibilidad de los conocimientos a través de un texto de carácter impreso, sin embargo, estas pretensiones de generalidad encontraron fuertes obstáculos, como los límites económicos y sociales. Precisamente estas dificultades han sido superadas ampliamente por los medios telemáticos que hacen posible la evolución y fusión de la telecomunicación y de la informática, sentando las bases para la sociedad intercomunicada² en los términos que la conocemos hoy en día.

¹ AGUILERA, Abel Téllez, "Nuevas tecnologías. Intimidad y Protección de Datos", Madrid, Edisofer, 2001, Pág. 22.

² SANZ – MAGALLÓN, José María, "¿Qué es la Sociedad del Conocimiento?", en Nueva Revista de Política, Cultura y Arte, Pág. 9, Madrid, 2000.

Este proceso acarrea drásticos cambios, de naturaleza política, social, laboral, cultural y antropológica, surgiendo beneficios y peligros asociados a estas rupturas en nuestra forma de concebirnos. No nos parece ajena la posibilidad de una futura democracia electrónica, la formación de innumerables comunidades virtuales que agrupen los más diversos intereses, la masificación del contrato electrónico, el incremento del teletrabajo, la televigilancia y muchos otros fenómenos vinculados a la sociedad informatizada.

Desde hace algunos años han quedado en evidencia, los riesgos asociados a esta sociedad de la información ya que numerosas actividades de nuestra vida diaria quedan registradas en diferentes ficheros de información, que al ser unificados permiten formar perfiles completos de los ciudadanos.

La tecnología ha implicado una mutación bastante importante en las tareas del Estado, pues la concepción de un Estado social derivó en un aumento gradual de las necesidades de información. La tecnología se comienza a vislumbrar como un verdadero poder, materializado en las diversas posibilidades de desarrollo y control sobre los individuos partes de la nación.

Así, la tecnología ofrece una gran capacidad de tratamiento y trasmisión de información. Precisamente esto es lo que vivió Francia hace ya treinta y nueve años. El Instituto Nacional de estadística elaboró el Proyecto SAFARI (*Système Automatisé pour les Fichers Administratifs et le Répertoire des Individus*) con el que se proyectaba instaurar un sistema de atribución de un número de identificación único para cada ciudadano, interconectando todos los ficheros administrativos.

El proyecto generó una amplia oposición por parte de determinados sectores políticos, medios de comunicación y sectores de la opinión pública, lo que determinó su posterior abandono.

Sin embargo, la conmoción ya estaba plasmada en la sociedad francesa. Se comprende que la sociedad informatizada es efectivamente la consecuencia necesaria del avance tecnológico pero se toma conciencia de la orientación futura que se adopte depende del equilibrio en los poderes estatales y la consolidación de la sociedad civil, siendo la informática, uno de los principales ingredientes en esta ponderación de intereses.

En efecto, quedó en evidencia que la capacidad de registro de las computadoras, el increíble aumento en la velocidad de consulta en la transferencia de la información y su respectiva cobertura, provoca para quien la posee un poder con límites poco demarcados.

Un caso similar ocurrió en Estados Unidos alrededor de 1972, cuando la sociedad de información comercial *R.L. Polk de Detroit*, almacenó datos personales sobre ciento treinta millones de ciudadanos, datos que reorganizados a través de un tratamiento informático, podían generar ficheros completos cuyo contenido tomaría en cuenta miles de aspectos diferenciados de los individuos.

Un tercer caso surgió en Alemania, entre 1982 y 1983 cuando la Ley del Censo de la Población, planteó la realización de una encuesta a todos los ciudadanos, solicitando numerosos datos, entre los que se encontraban:

- Nombre, apellidos, domicilio, teléfono, sexo, día de nacimiento, estado familiar, pertenencia legal -o no- a una asociación religiosa, nacionalidad.
- Datos sobre el uso de la vivienda (dimensión, mobiliario, clase de calefacción, número y uso de las habitaciones, renta mensual de las viviendas arrendadas, etc.), los medios de vida, la ocupación profesional o doméstica, y datos de formación académica
- Medio de transporte empleado y tiempo invertido en el viaje al centro de trabajo o centro de enseñanza, entre otros datos.

El objetivo de esta ley era la correcta definición de las políticas sociales y económicas y la correcta planificación de las inversiones de la Administración Pública, así como la

producción de material demográfico para los análisis estadísticos. Sin embargo, su promulgación, provocó en amplios sectores de la población un sentimiento de intranquilidad y desconfianza ante lo que se consideraba una grave infracción de los derechos fundamentales.

En efecto, a pesar de la obligatoriedad de anonimizar los datos para fines estadísticos, el tratamiento de la información recopilada conllevaría a una sencilla e inevitable disposición de toda la información personal de cada individuo, tornándolo en un “hombre de cristal”. Adicionalmente, el mezclar en la misma encuesta datos de empadronamiento y datos con fines estadísticos era una perversión del origen del censo como estadística descriptiva.

Ese mismo año, se presentó un recurso de inconstitucionalidad, que concluyó en una Sentencia del Tribunal Constitucional Alemán en la que se consideraban inconstitucionales algunos artículos de la Ley del Censo, y lo que es más relevante, se definía un nuevo principio conocido como “autodeterminación informativa”, que garantiza la facultad del individuo de decidir por sí mismo sobre la difusión y utilización de sus datos personales.

Desde hace décadas los organismos públicos y privados han tomado conciencia respecto a que la posesión de información construye poder en todos los campos del quehacer humano. De aquí que se entienda que la informática nace como necesidad del “manejo” de la información³, en cuanto al almacenamiento, uso y control de los datos recopilados.

Lo cierto es que no sólo los entes públicos y privados utilizan los beneficios de la era informática, sino muy por el contrario, desde los escritores más autodidactas hasta las microempresas, recurren al uso de las nuevas tecnologías y la información automatizada.

³ ORTÍZ ORTÍZ, Rafael, Hábeas data: derecho fundamental y garantía de protección de los derechos de la personalidad, Caracas, 2001, Pág. 6.

Sin embargo, la recogida y almacenamiento de datos personales no son actividades del todo novedosas. Antes del advenimiento de la sociedad de la información ya existían ficheros manuales que comenzaban a presagiar los riesgos que generarían para las personas los registros, como por ejemplo aquellos derivados de la inclusión de datos incompletos, falsos o datos manipulados para un fin diferente del que fundamentaba su recogida. No obstante, estos riesgos asociados a procedimientos manuales difieren mucho en cuanto a la escala de potencialidad dañosa que arraiga la evolución de la informática.

El progreso y desenvolvimiento de las novedosas tecnologías ha hecho posible un incremento de la posibilidad de almacenamiento y control de la información de dimensiones impensadas. A su vez, el proceso se acelera y se torna más violento con la aparición de modalidades de transferencia, acopio y utilización que se caracterizan por su agilidad y efectividad.

Las personas se difuminan en centenas de datos que posteriormente serán observados por otros sujetos que operan desde el anonimato acumulando información ilimitada de aspectos de la vida cotidiana de los individuos, en cuanto a salud, ideas políticas, creencias religiosas, aspectos económicos, etc.

La progresiva destrucción de la esfera íntima del individuo se comienza a concretar cuando los planificadores que han recogido toda esta información deciden sentarse a reflexionar para qué podrían utilizar todos estos datos. Los bancos de datos han preparado listas de los ciudadanos con sus datos respectivos, que de alguna manera podrían proyectar recelos en cuanto al uso que se haga de dicha información.

De aquí, que se promueva la promulgación de una serie de disposiciones legales encaminadas a reglamentar los aspectos más apremiantes de esta tensión entre la actividad informativa, el control de los poderes públicos y de los entes privados y la simultánea defensa de las garantías y libertades individuales con el objeto de asegurar el control democrático y el ejercicio social de la tecnología informática, impidiendo que

ella pueda transformarse en una verdadera amenaza al Derecho, a la intimidad, la vida privada y, en general, a los derechos de la personalidad.

Hace más de treinta años podíamos vislumbrar el panorama del futuro e intentábamos dotarnos de instrumentos vinculantes que mitigaran los riesgos asociados al desarrollo tecnológico, sin embargo, el proceso está en constante dinamismo. Pocas ramas de la ciencia sufren cambios tan continuos y drásticos y, ante todo, nunca estas mutaciones habían generado una repercusión tan grande en la sociedad, sin posibilidad de presentar marcha atrás.

En este contexto, la tarea de establecer filtros, contrapesar, interpretar y reestructurar información se convierte en una actividad estratégica que requiere una regulación adecuada que fije estándares de comportamiento y de disposición de aspectos técnicos. Esta materia se ha transformado en un gran desafío para las legislaciones nacionales, por la heterogeneidad en las ramas que se relacionan, procurando incorporar de la mejor forma estos nuevos valores y criterios, muchas veces ajenos al derecho, imponiéndose la tarea de conseguir que los avances tecnológicos sean dominados por el hombre y puestos al servicio de su perfeccionamiento⁴.

Paulatinamente los distintos países del orbe, en especial los europeos, han promovido el desarrollo de una nueva disciplina jurídica llamada Derecho Informático o de las Nuevas Tecnologías de la Información y Comunicación, que dada su naturaleza está supeditada a un constante desarrollo pero que pretende permanecer en persistente movimiento para abarcar los nuevos desafíos que vaya planteando esta sociedad informatizada.

En definitiva, la revolución científica y tecnológica nos ofrecerá una gama de ángulos y perspectivas de análisis muy distintos. Es decir, aquí se plantea el problema de

⁴ TRUYOL Serra, Antonio, "Bases filosóficas y metodológicas para un derecho de la sociedad de la información" en la obra colectiva Implicaciones socio-jurídicas de las tecnologías de la información, Madrid, CITEMA, 1991, pp139-143.

discernir como equilibrar estos avances con lo que pareciera ser más importante: el ser humano y sus derechos a la personalidad pues la informática y sus herramientas tienen que estar al servicio de los hombres y las mujeres y, no inversamente.

Por esta razón es tan importante un cambio de actitud frente a los nuevos instrumentos tecnológicos, dejando de lado aquella visión puramente técnica que exalta las capacidades del computador en comparación con la máquina humana. El énfasis debe radicar en los graves riesgos para los ciudadanos centrados en que el control y el manejo inadecuado de la información pueden limitar seriamente la participación social, económica e incluso democrática de los individuos, llegando al punto de una eventual marginación de la persona de la sociedad.

1.2. Procesamiento de datos y tratamiento de datos personales.

En las últimas décadas, con la llegada de los computadores como extraordinarias máquinas de cálculo que realizan procesos mecánicos a velocidades sorprendentes, se ha generado una revaloración de la información, su suministro y su uso en prácticas de variada naturaleza. Contar con información precisa, acertada y de calidad para el respaldo en la toma de decisiones es una prioridad en la sociedad de hoy en día.

En concordancia, un dato aislado no es sustento suficiente. De aquí que surja la creación de registros o bancos de datos, como conjuntos organizados de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización que permitan relacionar datos entre sí, así como realizar todo tipo de tratamiento.

A través de los registros de datos, se compilan uno a uno los datos personales aislados de una determinada persona, los que conglomerados permiten establecer determinado perfil del individuo, constituyendo aquella información de relevancia para la toma de decisiones.

Frecuentemente, datos, información⁵ y conocimiento son conceptos que se prestan para confusión. La “información” que consideran las casas comerciales es aquella contenida en bases de datos comerciales que entregan a los abonados datos precisos respecto a las áreas de interés. Sin embargo, en este caso se confunde el dato con la información.

Cuando estas bases de datos se transan en el mercado como fuente de conocimiento lo que se está comercializando son realmente datos en la forma de una serie de antecedentes numéricos y de texto.

La relación lógica que debería establecerse entre estos datos y el correlativo conocimiento, no siempre se cumple a cabalidad. El computador no permite por sí mismo establecer el planteamiento necesario para comprender un fenómeno, lo que evidencia que realmente el hombre no puede ser sustituido en los procesos de desarrollo de respuestas concretas para dar solución a un caso sino que, por el contrario, este conocimiento que se transa en el mercado sólo se produce como consecuencia del intercambio de ideas, interpretaciones y experiencia entre los seres humanos.

Datos e información son los términos que se prestan para más imprecisión. Ambos se utilizan para indicar todo lo que se transmite mediante la palabra, los diarios, libros, películas, etc. Sin embargo, en este caso debemos distinguirlos. Por un lado, el término datos se utilizará para hacer referencia a todo lo que se representa con alfabetos, números y cualquier otro signo o símbolo utilizado para transmitir un concepto⁶.

Para que los datos se transformen en información deben ser transmitidos a una persona o máquina con la finalidad de que esta los interprete otorgándole a los datos

⁵ COMISIÓN NACIONAL PARA EL MEJORAMIENTO DE LA ADMINISTRACIÓN DE JUSTICIA, Informática y derecho a la intimidad. Perspectivas de política criminal, Revista Judicial, Costa Rica Año XVI, N° 53, 1991, Pág. 136.

⁶ BING, JON, Derecho a la información: Una breve introducción, en Revista Ágora, N° 6, 1983, Pág. 35.

una forma, un contenido y una estructura que posteriormente pasará a constituir un conocimiento determinado, organizado y comunicable. De aquí que se afirme la existencia de una dependencia con el pensamiento humano⁷, que posibilita la indagación de datos y su consecuente valoración pues, en definitiva, serán los individuos los que decidirán qué hacer con la información que se posee.

Cabe ahora hacer referencia a qué es lo que podemos llamar dato personal. Un dato personal es básicamente cualquier información relativa a una persona, ya sea materializada en una imagen, un sonido, caracteres grafológicos, o incluso muestras físicas. Este es un concepto universalmente aceptado y las discrepancias en las legislaciones dirán relación, más bien, respecto de si las personas protegidas serán sólo las naturales y/o se admite la protección de las personas jurídicas⁸.

Así en nuestra Ley de Protección a la Vida Privada, se define en su artículo 2 letra f) como dato de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables⁹.

Esta definición es bastante parecida a la utilizada en la Ley Orgánica de Protección de Datos española que, en su artículo 3, define dato personal como cualquier información concerniente a personas físicas identificadas o identificables.

En definitiva, esta amplitud para definir dato personal no es una coincidencia. Un dato personal por sí sólo puede parecer totalmente inofensivo atendida la información simple, básica e inocua que entrega. Sin embargo, como explicábamos anteriormente, este dato junto a otros tantos de igual naturaleza son capaces de estructurar una compleja representación de la identidad de una persona.

⁷ COMISIÓN NACIONAL PARA EL MEJORAMIENTO DE LA ADMINISTRACIÓN DE justicia, Informática y derecho a la intimidad. Perspectivas de política criminal, en Revista Judicial, Costa Rica Año XVI, N° 53, 1991, Pág. 138.

⁸ A vía de ejemplo, la ley Argentina considera la protección de las personas jurídicas y el proyecto de ley en actual tramitación, en Chile, sigue la misma senda.

⁹ Ley N° 19.628 sobre Protección de la Vida Privada, Ministerio Secretaria General de la Presidencia, Santiago, Chile, 28 de agosto de 1999, Artículo 2 letra f).

Incluso, la misma referencia a personas identificadas o identificables hace hincapié no sólo en aquellos datos que se identifican con una persona directamente sino también a aquellos que pueden hacer potencialmente identificable a una persona, ampliando aún más el concepto.

Por lo tanto, son elementos integrantes de esta definición:

- i. Toda información: estamos ante un concepto amplio que incluye imágenes, sonidos, caracteres grafológicos o incluso muestras físicas que entreguen antecedentes de un sujeto.
- ii. Concerniente a personas naturales: en Chile, actualmente, las personas jurídicas no son sujetos de protección de datos personales pues se trata de un atributo de la personalidad que protege la intimidad y vida privada de las personas.
- iii. Identificada o identificable: se considerará, asimismo, dato personal aquel susceptible de ser enlazado a determinada persona mediante mecanismos de identificación.

Respecto a los tipos de datos personales podemos señalar que existen datos personales propiamente tales y datos personales sensibles. Éstos últimos son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías, las opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psiquiátricos y la vida sexual.

Otras distinciones que pueden realizarse atienden a si los datos son:

- a) Simples: entregan información básica de la persona.
- b) Compuestos: entregan información variada de la persona.
- c) Inocuos: datos que se consideran *a priori* inofensivos.

- d) Riesgosos: datos sensibles que reflejan ámbitos íntimos de la persona.
- e) Patrimoniales: datos que entregan información sobre la situación económica de una persona determinada o determinable.
- f) Positivos: datos que revelan información beneficiosa o ventajosa de la persona.
- g) Negativos: datos que revelan información perjudicial o crítica de la persona.

Por lo tanto, sintetizando, el dato personal hace referencia a cualquier información sobre una persona, independientemente del medio que se utilice para captarla, transmitirla, manejarla, registrarla, conservarla o comunicarla, independientemente también de la naturaleza de dicho dato, pues toda la información acerca de la persona, se considera dato personal.

Cabe señalar un punto importante. El tratamiento jurídico de la información recolectada sobre una persona no es igual en todos los casos y depende en gran parte de la naturaleza, riesgos o efectos que puedan provocar los distintos tipos de información personal que serán, en último término, los que determinen los parámetros a seguir en el tratamiento por terceras personas.

Este parámetro dependerá, asimismo, de los fines que se persigan con la recolección de datos, los que podrán ser lícitos o ilícitos. Serán lícitos cuando se busquen fines de seguridad nacional, tributarios, penales, comerciales, financieros, clínicos, laborales, estadísticos, encuestas, científicos, académicos, sociales, servicios públicos, delictivos, etc. Serán éstos los que justificarán el uso legítimo o ilegítimo de la información y la eventual negligencia o abuso en el tratamiento de los datos personales.

La forma en que la información de las personas es recolectada, almacenada, procesada, utilizada, divulgada y transferida configura las etapas en el tratamiento de los datos personales.

El primer aspecto al que debemos hacer referencia respecto al proceso de tratamiento de datos personales es la modalidad del procedimiento, la que puede ser no automatizada o automatizada.

El procedimiento será no automatizado cuando estemos ante un conjunto de datos de carácter personal organizados de forma manual y estructurados conforme a criterios específicos relativos a personas físicas, que permitan acceder con moderados esfuerzos a sus datos personales.

El procedimiento será automatizado cuando hablemos de todo conjunto de datos de carácter personal organizados de forma mecánica y determinados conforme a parámetros preestablecidos.

En nuestra legislación no se distingue si el tratamiento de datos es automatizado o no, de manera que nos basta, hasta este punto, con realizar la distinción. Sin embargo, debemos insistir que la invasión a la intimidad, privacidad y a los derechos de la personalidad se asocia a las nuevas tecnologías, todo ello impulsado por el hecho que el uso de instrumentos informáticos ha permitido que las empresas organicen estos datos, obteniendo perfiles completos de sus titulares.

Para nuestro propósito, lo importante es establecer que el tratamiento de datos está caracterizado por la existencia de un soporte físico en el que estén registrados estos datos, indiferentemente de la forma de tratamiento, es decir, sea manual o automatizada. La idea de la diferenciación es evitar que se eluda con relativa facilidad las obligaciones que persiguen garantizar un tratamiento adecuado de los datos que protejan los derechos fundamentales de las personas, por la vía de señalar que no se trata de un procedimiento automatizado.

Por lo tanto, el primer presupuesto necesario en el tratamiento de datos personales será un soporte físico materializado en la forma de un fichero, registro o banco de datos, conceptualizándose como el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de sus creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

Igualmente, la protección de los datos de carácter personal será aplicable a los ficheros públicos y a los privados. La naturaleza o calidad del responsable del fichero es indiferente en relación con la tutela de los bienes jurídicos protegidos.

Debemos tener en cuenta que el soporte físico será el resultado visible de todo un proceso. En efecto, en el tratamiento de datos personales se desarrollan las siguientes etapas:

i. Primera etapa: Recogida de datos.

Durante la etapa de recogida de datos se recopila toda la información circulante de una persona física determinada o determinable, ya sea por medios manuales y/o automatizados.

- Los datos podrán ser obtenidos directamente de la persona, de un tercero o a partir de otros sistemas de tratamiento de información.
- Los datos acopiados podrán ser de diversa naturaleza, podrán referirse a características físicas o morales de la persona o a hechos de su vida íntima, como hábitos personales, origen racial, ideologías, tendencias políticas, creencias religiosas, etc.

En esta fase de recopilación, se establecen los límites lícitos, los que pueden ser de origen subjetivo, es decir, aquel derivado del consentimiento del interesado, o de procedencia objetiva, según se excluyan ciertas categorías de datos por su calidad. Simultáneamente, se exige que estos datos sean ciertos, precisos, íntegros, obtenidos de acuerdo a la ley y en conformidad a las finalidades establecidas. En todas las legislaciones que cuentan con una normativa tendiente a la protección de datos personales se prohíbe expresamente la recopilación de datos sensibles con fines discriminatorios.

ii. Segunda etapa: Tratamiento propiamente tal.

En esta etapa se comienzan a estructurar los datos recogidos en torno a la organización de un registro o banco de datos, como un soporte material que dispone la ordenación de los datos personales recolectados. Aquí, la seguridad y la transparencia son requisitos fundamentales, la primera en cuanto debe garantizar el carácter secreto de la información obtenida, estableciéndose la necesidad de regular el derecho de acceso a los datos. Mientras, la transparencia es básica para controlar los procesamientos de datos personales.

En el tratamiento propiamente tal se pueden desarrollar las siguientes sub etapas:

- Registro: los datos recolectados son consignados en una unidad de almacenamiento.
- Organización: los datos consignados en la unidad de almacenamiento son coordinados bajo la forma de algún parámetro preestablecido.
- Conservación: los datos almacenados deben ser utilizados eficientemente, cautelando su veracidad y actualidad.
- Modificación: los datos erróneos deben ser modificados.
- Cancelación: los datos caducos o cuyo tratamiento carezca de fundamento legal deben ser cancelados.
- Bloqueo: los datos cuya veracidad no pueda ser establecida y a cuyo respecto no corresponda la cancelación, deben ser bloqueados.

iii. Tercera etapa: Consulta al registro o banco de datos.

Esta etapa se origina como resultado de todo el procesamiento. Durante esta fase cuando se pueden provocar graves violaciones a los derechos de la personalidad pues en este momento se decide con que finalidad se utilizarán los datos personales que constan en el banco de datos.

- Extracción: los datos personales podrán obtenerse desde el soporte físico con la finalidad de manifestar determinada correlación dentro de cierta proporción de datos.

Lo importante es no aislar los datos con la finalidad de detectar cierta tendencia, apartándolos de su marco contextual.

- Consulta: los datos personales serán buscados, examinados o inspeccionados para cumplir alguna de las finalidades trazadas para el tratamiento de los datos personales.
- Utilización: los datos consultados podrán ser empleados para los fines previstos, por ejemplo, para determinar la solvencia de un deudor.
- Comunicación por transmisión: consiste en la transferencia de los datos personales recolectados de un sujeto a otro. Es decir, es la actividad a través de la cual terceros, distintos del titular, toman conocimiento de los datos personales.
- Difusión: propagación de los datos personales a terceras personas.
- Cualquier otra forma que facilite el acceso a los datos o a la información elaborada a partir de ellos.

iv. Comunicación de datos.

Esta etapa tiene sólo un carácter eventual, es decir, no está presente en todos los procedimientos de tratamiento de datos personales, sin embargo, cuando ocurre puede ser uno de los momentos más delicados del proceso de tratamiento de datos pues en este lapso es cuando puede producirse un esparcimiento de la información.

La transmisión entre naciones de la información de los individuos, almacenada en un registro de datos, supone un aspecto muy relevante en el estudio actual de la protección de datos personales. Ya hacia 1973 en Suecia,¹⁰ se estableció que para que se llevara a cabo esta operación debía contarse con la autorización especial del individuo¹¹. Este mismo año, en la Convención Internacional de las

¹⁰ Datalagen 1973, SFS 1973, núm. 289.

¹¹ CERDA Silva, Alberto, Mecanismos de control en la Protección de Datos Personales en Europa, en Revista *Ius et Praxis*, Derecho de la Región, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Talca, 2006, Pág. 223. "A través de esta ley, Suecia imponía un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control –la *Datainspektionen*, expresión del Ombudsman

Telecomunicaciones, en Malaga, se estableció el principio del flujo internacional de datos sin obstáculos ni interrupciones, estableciéndose una garantía de seguridad y secreto para los datos transmitidos. El problema que se presenta en esta etapa radica en las desiguales condiciones de tratamiento de datos en los distintos países del mundo, razón por la cual fue necesario, siete años más tarde, que la Convención Europea estableciera que la libertad de transferencia de datos está condicionada por la equivalencia de protección de datos entre los países parte de la transmisión.

1.3. Potencialidad dañosa que arraigan los registros de datos personales.

Hasta aquí hemos dado noticia de algunos antecedentes históricos relativos al tratamiento de datos personales y como se desarrolla este procesamiento de datos, sin embargo, la real magnitud de la problemática será entendida cuando la sociedad tome conocimiento de la incalculable e ilimitada potencialidad dañosa que se arraiga en los bancos de datos.

Los perjuicios que pueden provocarse a través de la utilización de registros de datos personales no consisten únicamente en aquellos que se derivan del registro de datos falsos o erróneos, del uso de éstos para fines discriminatorios, de su cesión contraria a la ley, etc. Es muy difícil predecir con exactitud cuáles serán los posibles daños que llegaran a generarse con estas nuevas herramientas, puesto que nunca sabremos a ciencia cierta cuál será el uso que se les dará en definitiva.

Por el momento podemos señalar los instrumentos tecnológicos que manifiestan la mayor capacidad perniciosa en la utilización de bancos de datos:

1.3.1. Mega-archivos:

proyectado al tratamiento de datos personales- que vela por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones”.

A través de las bases de datos informatizadas se proporciona un veloz almacenamiento, tratamiento y recolección de la información archivada, viabilizando la clasificación de los datos y, simultáneamente, la categorización de los sujetos titulares de la información. Conjuntamente, se produce un rápido entrecruzamiento de la información almacenada, creando archivos gigantes o mega – archivos, que contienen innumerable información respecto de muchas personas¹², la cual habrá sido recogida desde diferentes bases de datos.

Con inusitada celeridad se procederá a enlazar los datos para ser utilizados con finalidades ajenas a aquellas presupuestadas en el momento de acopio de datos. Por ejemplo, con datos crediticios, judiciales, policiales, clínicos o datos provenientes del registro de las tarjetas de crédito se podrá perseguir fines de marketing, tratando incluso datos sensibles o confidenciales.

Se permitirá entonces generar distintas clasificaciones de los individuos utilizando sus datos arbitrariamente, llegando incluso a ejercer medidas discriminatorias contra los titulares de los datos con total prescindencia de su conocimiento.

Estos cruces, imposibles de hacer cuando los datos se consignaban en papel o eran procesados con sistemas informáticos más precarios, se realizan cada vez más, tanto en organismos públicos como en empresas privadas¹³. De aquí la desconfianza que debe suscitarse en la estructura social, en las legislaciones de todos los países desarrollados y en las conductas individuales, ante la vulneración de los derechos de la personalidad.

1.3.2. Data Warehouse:

¹² BOLOTNIKOFF, Pablo, Informática y responsabilidad civil: contratos informáticos, bases de datos, nombres de dominio de Internet, contenidos ilícitos en Internet, contratación electrónica y firma digital, 1° Edición, La Ley, Buenos Aires, Argentina, 2004, Pág. 107.

¹³ FORD, Anibal, La marca de la bestia. Identificación, desigualdades e infoentretenimiento en la sociedad contemporánea, Buenos Aires, Grupo Editorial Norma, 1999, Pág. 195.

Aunque el término no puede ser traducido con exactitud al español, en su traducción más literal sería “almacén (*warehouse*) de datos (*data*)”, mientras Aníbal Ford prefiere usar el término “bodega de datos”¹⁴.

La revolución que han producido los medios digitales trajo consigo una modificación en la conceptualización del concepto de almacenamiento y procesamiento de datos. Las compañías se han hecho parte de este proceso desarrollando novedosas estrategias de gestión para competir en el mercado.

Precisamente, para el cumplimiento de estas finalidades, es decir, para maniobrar gran cantidad de datos en forma centralizada y conservar sus sistemas en línea, las empresas se han dotado del *data warehouse* y *data mining*, fenómenos que no han sido suficiente y específicamente regulados por el derecho.

El *data warehouse* es la nueva modalidad de almacenamiento y manejo de grandes volúmenes de información corporativa donde se integran todos los elementos para mejorar la toma de decisiones¹⁵. Dirigido al tema que nos concierne, se utiliza para emplear los datos recolectados en trabajos de *marketing*, investigación, localización de dificultades, etc., haciendo posible que la empresa se desenvuelva en el mercado de una forma más precisa, rentable y lucrativa.

Bell Inmon, considerado el padre de las bases de datos, definió en 1992 esta bodega o almacén de datos como una colección de datos orientados a temas integrados, no volátiles y variantes en el tiempo, organizados para soportar necesidades empresariales, estableciéndose como una fuente central de información que puede ser estandarizada y accedida desde distintos sistemas operacionales.

¹⁴ FORD, Aníbal, La marca de la bestia. Identificación, desigualdades e infoentretenimiento en la sociedad contemporánea, Buenos Aires, Grupo Editorial Norma, 1999, Pág. 195.

¹⁵ ORTÍZ Ortiz, Rafael, Hábeas data: derecho fundamental y garantía de protección de los derechos de la personalidad, Caracas, 2001, Pág. 12.

Para que el *data warehouse* este dotado de los medios necesarios para extraer la información, requiere al *data mining* como herramienta metodológica que convierta los simples datos en conocimiento mediante la aplicación de ciertos algoritmos que permiten revelar relaciones ocultas, patrones y tendencias de comportamiento entre los mismos, de manera que este conocimiento se aplique a la resolución de problemas.

Por muy útiles que parezcan, estas herramientas arraigan una gran potencialidad perniciosa. Lo realmente amenazante es el hecho de que en el análisis de los bancos de datos se busquen las valiosas “pepitas de oro”¹⁶ que posibiliten dirigirse al blanco preestablecido, respondiendo preguntas como ¿Qué productos adquiere determinado segmento de gente? ¿A qué clientes apunta determinada publicidad? ¿Qué tipo de clientes pueden ser seducidos por la publicidad de la competencia?

Debe reconocerse, sin embargo, que estas herramientas pueden ser utilizadas de una forma beneficiosa para la sociedad. Por ejemplo, la empresa de electrodomésticos estadounidense *Whirlpool* utiliza su *data warehouse* para realizar un seguimiento a sus clientes y productos, haciéndose factible que en caso de fallas en los electrodomésticos se detenga la producción y se otorgue una solución a los clientes que ya cuentan con el producto. Precisamente, esto fue lo que ocurrió en 1993 cuando se detectó una falla técnica en una manguera de conexión de una lavadora, identificando a los clientes y reparándoles el equipo antes de que se produjera la falla.

No obstante, consideramos que este caso es una excepción a la regla, lo normal es que estos instrumentos se utilicen para finalidades poco transparentes. Ya se está haciendo habitual la práctica de *target marketing* y *cross marketing*, que se utiliza para realizar seguimiento de tarjetas de crédito y análisis de riesgo crediticio mediante el almacenamiento de tendencias y relaciones a partir de la información detallada de éstas. La idea es determinar quiénes poseen mayor probabilidad de adquirir determinado producto o servicio del banco, llegando a los clientes que realmente se

¹⁶ FORD, Aníbal, *La marca de la bestia. Identificación, desigualdades e infoentretenimiento en la sociedad contemporánea*, Buenos Aires, Grupo Editorial Norma, 1999, Pág. 195.

quieren captar, ofreciéndole a cada uno los productos que considera que se ajustan a su medida.

La finalidad de este ejercicio es captar el grupo objetivo hacia el cual está dirigido determinado bien del mercado, designando el destinatario ideal de la campaña, producto o servicio.

Las empresas buscan dominar las actitudes de un *target* frente a las campañas, los productos o los servicios y los diferentes medios de comunicación, puesto que hace más posible acercarlos y dirigirse con el mensaje apropiado, optimizando el reintegro de la inversión concretada en ganancias.

Así, uno de los ejercicios típicos para el cumplimiento de este objetivo es clasificar las variables demográficas, sociográficas, económicas, etc. del consumidor, examinando sus características, motivaciones y acciones intentando representar la mente del individuo.

La imposibilidad de conocer el mercado y sus actores implicaría tomar decisiones con un costo financiero más alto, sin certeza de retornos. De aquí que se impulse desenfrenadamente la indagación ilimitada en el perfil de los humanos como consumidores.

El problema es que estas actividades se realizan de forma encubierta con prescindencia absoluta del consentimiento de cliente, priorizando únicamente la obtención de recursos y legitimándose a través de las correspondientes debilidades en los sistemas normativos nacionales.

1.3.3. Datavigilancia:

Según Roger Clarke la datavigilancia es el uso sistemático de bases de datos personales en la investigación o monitoreo de las acciones o comunicaciones de una o más personas.

Nunca, hasta ahora, se habían alcanzado niveles tan elevados de formalización social, mirados desde su realidad hacia su potencialidad. Este contexto se ve reforzado por el avance progresivo de los distintos sistemas informáticos de recolección, análisis y entrecruzamiento de información de distinto origen, que enmarcados en este fenómeno tienen como objetivo observar, tipificar y controlar a las personas, sus acciones y sus procesos sociales

Luego, es cierto que la datavigilancia, en una de sus caras, hace más amigable el acceso a bienes, servicios y espacios, optimizando la eficiencia, comodidad y racionalización de los recursos pero al mismo tiempo provoca nuevas formas de discriminación y también genera nuevas formas de segregación y distinción social.

Por lo tanto, al margen de los beneficios que podríamos cuantificar, estos procesos implican un fuerte atentado contra la privacidad individual, contra la creatividad y la crítica social al construir perfiles, categorizaciones y reducciones simplificadas de las personas.

La datavigilancia intenta la formalización de lo supuestamente no formalizable: la diversidad de las identidades individuales y socioculturales. Y reduce esas identidades a un conjunto – necesariamente finito y arbitrario – de registros y campos de datos¹⁷.

Los mecanismos de datavigilancia pueden ser utilizados para finalidades muy diversas que pueden ir desde la configuración de perfiles para actividades de *marketing*, examen de la conducta de las personas frente al consumo de productos y servicios, llegando incluso a utilizarse para crear estereotipos de la gente con fines derechamente discriminatorios.

¹⁷ BOLOTNIKOFF, Pablo, Informática y responsabilidad civil: contratos informáticos, bases de datos, nombres de dominio de Internet, contenidos ilícitos en Internet, contratación electrónica y firma digital, 1° Edición, La Ley, Buenos Aires, Argentina, 2004, Pág. 111.

El problema más importante en la datavigilancia radica en el contrapeso constante de intereses que se da en esta área. En efecto, desde el 11 de septiembre de 2001 la libertad de los ciudadanos se vio comprometida en la lucha contra el terrorismo, los individuos transaron la intromisión en derechos de su personalidad con el objetivo de ganar seguridad, propiciándose la creación de herramientas de vigilancia capaces de analizar, simultáneamente, innumerables comunicaciones telefónicas y correspondencia vía correo electrónico.

La facultad de rastrear los datos de cualquier sujeto, a través de la invasión en los registros que arrojan las actividades diarias en diferentes sistemas informáticos lleva a conceptualizar a la datavigilancia como una subyugación personal que intercambia privacidad y libertad individual por seguridad pública.

Precisamente, uno de los obstáculos que encuentra la protección a los datos personales radica en el relativismo que se le otorga constantemente. A veces puede priorizarse la seguridad pública, el combate a los actos criminales o la rapidez en las transacciones.

Mega – archivos, *data warehouse* o datavigilancia se utilizan para fines de orden público que el Estado aprueba, o bien, los mismos ciudadanos incentivan a través de diversos servicios, sin profundizar en las consecuencias que se pueden desprender de estos procesos.

Es difícil pensar en una nación que no promueva como uno de sus objetivos primordiales la consolidación de la seguridad en la sociedad. Así, se plantea a nivel mundial la lucha contra la delincuencia, permitiéndose pesquisas e indagaciones jurídico penales con amplios márgenes de libertad.

Los modernos medios de intervención, en aras del afianzar el resguardo ciudadano, permiten la intervención secreta en las actividades de las personas, valiéndose de los instrumentos tecnológicos actuales. De esta forma, se impulsa a una importante

recolección de datos y generación de información, lo que se traducirá en un aparataje investigativo que la persona es incapaz de percibir.

De esta forma, se permite la vigilancia del tráfico telefónico, la amplia búsqueda de rastros a través del contraste entre grandes cantidades de datos, observaciones policíacas a mediano y largo plazo, utilización de agentes encubiertos, escucha de conversaciones por medio de micrófonos, etc.

Efectivamente si estos medios conducen a la detención de un peligroso delincuente, la sociedad aplaude la astucia de aquellos involucrados en la investigación, sin embargo, cuando el sujeto investigado es inocente ¿en qué posición quedan sus derechos tras la utilización de estos medios de control de alto espectro? Probablemente en este caso el derecho a la protección de datos personales tiene pésimas oportunidades pues una vez más se está transando parte de la esfera propia de los derechos de la personalidad por seguridad.

Ahora veamos otro caso. Otro ejemplo de amenaza a los derechos fundamentales producto del desarrollo de la tecnología se materializa en el fenómeno de peaje electrónico. Su punto de partida es el interés del Estado o de aquellas sociedades privadas interesadas en atender o encargarse de las carreteras de larga distancia, de forzar a los usuarios de estas carreteras a pagar una tasa o peaje¹⁸.

Este mismo objetivo podría ser logrado con centros de peaje o con sistemas de pago anticipado que no implicarían mayores conflictos de intereses. Sin embargo, en la actualidad son frecuentemente utilizados los sistemas de pago posterior (*post-paid-systems*). Estos sistemas utilizan las nuevas tecnologías para su desarrollo ya que están diseñados de manera que los vehículos envían determinadas informaciones a las máquinas que están ubicadas en distintos segmentos de la vía y en tramos específicos

¹⁸ HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 44.

se le cobra al usuario, emitiéndose una cuenta al final del mes con el total de los cobros registrados por las máquinas.

Aunque las personas no se planteen en el día a día como estos mecanismos podrían vulnerar su derecho a la protección de datos, es posible afirmar que constituyen potenciales ataques informativos para las personas. Podemos pensar en la hipótesis que frente a un débil sistema de protección de datos personales se evalúen los datos, provenientes del cobro de peaje, para finalidades distintas al simple cobro de la tasa por el uso de la vía, llegando a manos de terceros los movimientos espaciales exactos que realiza determinado individuo.

Es importante reconocer que entre menos datos sean recogidos menor será la posibilidad de vulneración a los derechos de la personalidad, lo que no implica en forma alguna que se opte por impedir las innovaciones, sino que sólo se establece la urgente necesidad de establecer límites.

El último caso al que haremos referencia proviene del área de la salud. En ciertos países por políticas de salud se utiliza la tecnología para proveer a los ciudadanos de una herramienta que hace más expedito y económico el funcionamiento de la administración y, simultáneamente, posibilita una rápida provisión de datos concernientes a los individuos. Se trata de tarjetas – chip o tarjetas de salud para los asegurados por enfermedad, las que en un pequeño espacio aglomeran los datos médicos relevantes de cierta persona, permitiendo una pronta consulta.

Se hace posible simplificar en gran medida la información médica de una persona, sin embargo, es difícil predecir el nivel de la amenaza si esta tecnología es utilizada de manera incorrecta. Es tal la cantidad de datos personales e íntimos que se contienen en esta base de datos que por esta vía podría construirse un perfil del ciudadano que, por ejemplo para empleadores y aseguradoras¹⁹ permitiría ejercer fuertes

¹⁹ HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 48.

vulneraciones en los derechos del individuo, en especial a través de actos discriminatorios.

Es de fundamental importancia que en estos casos el consentimiento del interesado hacia la obtención de la tarjeta y su uso no se entienda como un consentimiento “puro”, es decir, como una aprobación amplia que avale todos los ejercicios que se realicen con la tarjeta. El acceso a la tarjeta se debe restringir hacia lo “necesario”, asegurando que el individuo sepa con certeza cuáles informaciones sobre él se encuentran contenidas en el chip, y quién y cuándo podrá leer las informaciones insertas en ella.

Estos ejemplos han sido abordados para ilustrar en algún grado la debilidad que subyace al derecho cuando no está dotado de las herramientas necesarias para hacer frente a los avances tecnológicos. El uso de nuevas y más avanzadas modalidades de *software* y *hardware* no implica únicamente una simple intrusión en los datos de una persona, sino que proyecta una apertura masiva de aspectos múltiples de la vida de los individuos.

Si a través de estos mecanismos se permite crear perfiles y hábitos de consumo para conducir mejor la publicidad, se vislumbran fundamentos positivos. Sin embargo, si lo que se pretende es advertir las debilidades del público y mediante esta información proceder a explotarlos, queda de manifiesto uno de los tantos fundamentos negativos que podemos observar en las conductas de los titulares de los bancos de datos y que hacen tan necesaria y perentoria una regulación adecuada del mercado actual de la información.

1.4. Aproximación a los derechos fundamentales vulnerados en el proceso de tratamiento de datos personales y supuesta contraposición con los principios de necesidad de información, libre circulación de información y derecho de información.

Uno de los objetos de estudio del Derecho Informático consiste en determinar las incidencias que tienen las nuevas tecnologías en los derechos de las personas, en especial en los derechos de la personalidad y su susceptibilidad de vulneración.

Efectivamente el ser humano es un ser social por naturaleza, pero asimismo necesita desenvolverse en su vida interior, ajeno a las relaciones que sostiene con otros individuos, de modo de alcanzar el desarrollo de su libertad individual.

La sociedad de la información permite que las personas se hagan presentes en los medios anónimamente, no obstante, de forma paralela, el tratamiento de datos y su circulación, implican una exposición de la vida privada de las personas. No en vano, las Constituciones de numerosas naciones democráticas del mundo han asegurado a todas las personas el respeto y la protección a su vida privada y pública y a la honra de su persona y su familia, así como la inviolabilidad del hogar y de toda forma de comunicación privada, instaurando estos principios como fundamentos del orden político y la paz de la comunidad.

Cuando nos planteamos el desafío de definir qué derechos son susceptibles de ser vulnerados a través del tratamiento de datos personales pensamos en primer término en nuestra intimidad y vida privada. Conceptualizar lo que es intimidad y sus alcances ha sido una ardua tarea para numerosos autores, especialmente por el rol instrumental que juega este concepto.

Sin embargo, al profundizar en la serie de vulneraciones que pueden derivarse del procesamiento de datos personales se percibe que sostener que el derecho a la intimidad ha sido infringido puede implicar la vulneración de otros tantos derechos del individuo, como el derecho a la vida, el derecho al trabajo, el derecho a la educación, el derecho a la salud, etc.

El tratamiento de datos personales en la sociedad de la información, no puede limitarse únicamente a la intimidad y su posibilidad de vulneración, sino que se involucra una serie de otros derechos que pueden estar contemplados también como derechos

fundamentales, o bien, pueden considerarse derechos de menor rango, o incluso, pueden ser nuevos derechos aún en desarrollo, no incluidos a nivel constitucional.

Por ejemplo, durante el gobierno militar se recolectó numerosa información de las personas, proveniente de diversas fuentes, en especial en lo que respecta a su ideología. El uso que se dio a esta información es de público conocimiento, afectándose el derecho a la vida.

Otro caso quedó en evidencia hace algunos años. DICOM, empresa que ofrece bases de datos a sus clientes, registró las deudas de numerosas personas, formando una lista de morosidades ampliamente consultada por muchas empresas. Varias personas cuyas deudas estaban efectivamente pagadas, no fueron retiradas del listado, haciéndose una practica habitual exigir a los postulantes a trabajos no estar enlistados en DICOM, de manera que se les excluía de proceso de solicitud de forma automática. Aquí se afectó el derecho al trabajo.

Una Clínica, procesa en bases de datos las enfermedades de los pacientes atendidos, entregando dicha información a las ISAPRES. Una familia acude a una ISAPRE, solicitando registrarse como afiliado. La solicitud se deniega porque la familia verifica una tendencia a presentar graves enfermedades cardiovasculares. Aquí se afecta el derecho a la salud.

Esta interrelación del derecho a la intimidad y una serie de otros derechos, deja en evidencia que el derecho a la intimidad y el derecho a la privacidad, frente al tratamiento de datos personales no son derechos suficientes para la sustentación de un sistema de protección de datos personales.

Las limitaciones con que se encuentra el término intimidad y privacidad son de diversa índole. Una de ellas radica en la dificultad de definir estos términos, complejidad que se produce por el fuerte contenido emocional asociado al término, por los constantes cambios en los modos y costumbres de la sociedad o quizás porque en el intento de definirlo semántica y etimológicamente es inevitable alcanzar sólo una concepción

restringida y limitada que incorpore únicamente las manifestaciones más reservadas del comportamiento individual y familiar²⁰.

Señalamos, asimismo, que el derecho a la intimidad y a la vida privada no consigue abarcar la serie de derechos que pueden llegar a ser vulnerados a través del procesamiento de datos personales. Sin embargo, su mayor debilidad se encuentra en las defensas que se otorgan frente al quebrantamiento del derecho a la intimidad. Muchas veces sólo tras la vulneración se puede esgrimir un derecho a excluir del conocimiento ajeno ciertas informaciones concernientes a la persona y no se otorga un derecho previo a controlar la información personal que constituirá una protección mucho más adecuada y eficiente.

Al afirmar que estos conceptos son insuficientes para alzarse como los bienes jurídicos exclusivos sobre los que gravitará el derecho a la protección de datos de carácter personal, de forma alguna pretendemos despojarlos de la importancia que se les ha atribuido. Por el contrario, efectivamente son el presupuesto básico histórico sobre el cual se ha desarrollado el reconocimiento de la protección a los datos personales y es por esta razón que dedicaremos el próximo capítulo para ilustrar en qué forma se han desarrollado y cómo se ha evolucionado hacia el nacimiento de un nuevo derecho capaz de congregar todos los elementos que requieren protección frente al procesamiento de datos personales.

Explicaremos como la construcción del concepto de autodeterminación informativa comienza a establecerse a través del contraste entre los ámbitos de protección. Efectivamente, intimidad y vida privada poseen un núcleo esencial conformado por los aspectos más próximos a las personas y que representan su libre desarrollo. En tanto, la transición hacia la autodeterminación informativa se realiza al poner énfasis en los aspectos más extensivos de la protección que se identifican con aspectos de la vida de

²⁰ MARTÍNEZ Martínez, Ricardo, "Una aproximación crítica a la autodeterminación informativa", Thompson Civitas Ediciones, Madrid, 2004, Pág. 34.

las personas que no afectan necesariamente su interioridad y que cada individuo decide mantener en reserva.

Precisamente “la decisión de mantener en reserva” constituye el carácter fundamental de la autodeterminación informativa, como la facultad de los individuos de decidir por sí mismos, sin intromisiones ajenas, en qué momento y con qué limitaciones procederán a revelar información de carácter personal.

Cabe advertir que este derecho no es absoluto, sino que tiene sus restricciones para hacerlo compatible con los intereses de la sociedad y los derechos de terceras personas, pues la finalidad de la protección de la autodeterminación informativa no pretende entorpecer la circulación de datos, sino que establecer una estructura adecuada para esta práctica, asegurando condiciones y estándares de calidad adecuados.

Esta necesidad de equilibrio se percibe precisamente en la concepción de que el derecho a la protección de datos personales ha surgido como consecuencia de la idea de la información como un elemento imprescindible en el desarrollo del individuo. Se ha percibido que el moderno procesamiento de datos puede delinear estructuras y pintar cuadros que por medio de la simple utilización de la vista del observador nunca hubiera sido posible poner en conjunto²¹, aportando elementos que permiten orientar la acción de los seres humanos en la sociedad.

Existe una esta falsa percepción que afirma que los principios de necesidad de información, libre circulación y derecho a la información se contraponen a un derecho a la protección de datos personales porque justificarían a toda costa la recolección de información de toda índole.

²¹ HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 6.

En efecto, el derecho a la información nace oficialmente con la Declaración Universal de Derechos Humanos, de 1948. Su artículo 19 establece que.

“Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

En consecuencia el contenido del derecho a la información se puede dividir en tres grandes facultades o derechos, a saber: la de recibir, la de difundir y la de investigar informaciones²². Así, la facultad de recibir información se refiere a la prerrogativa que tiene todo ciudadano de recibir noticias y opiniones que se pudieran transmitir. Mientras, la facultad de difundir información se construye sobre el fundamento de que los múltiples medios de comunicación y la divulgación de las noticias de relevancia pública, favorecen el pluralismo democrático y fomentan un amplio debate para que la ciudadanía participe abiertamente.

Por último, la facultad de investigar información es la prerrogativa atribuida a los profesionales de la información, a los medios informativos en general y al público de acceder directamente a las fuentes de informaciones y de las opiniones, y de obtener éstas sin límite general alguno, facultad que debe considerarse en su doble faceta, es decir, como derecho del ciudadano y como deber de los que manejan las fuentes de información²³.

En consecuencia, la necesidad de información, su libre circulación y el derecho a la información promueven que el acceso a la información sea una instancia necesaria de participación ciudadana y la protección de los derechos vinculados, pues sin

²² ARMAGNAGUE, Juan, Derecho a la información, Hábeas Data e Internet, Buenos Aires, Ediciones La Roca, 2002, Pág. 165.

²³ DESANTES, Guanter, José María, La información como derecho, Madrid, Editorial Nacional, 1974, Pág. 31.

información adecuada, oportuna y veraz, la sociedad difícilmente se encontrará en condiciones óptimas para participar en la toma de decisiones públicas.

De aquí que se cautele la utilización racional y productiva de la información en beneficio del individuo y de su comunidad y no como herramienta capaz de vulnerar los derechos de las personas.

Entonces, estos principios y derechos que parecieran antagónicos a la protección de datos personales, realmente integran su contenido. El derecho a la información es - en relación a los datos sobre la propia persona - una parte clásica de cualquier derecho a la autodeterminación informativa²⁴ y un presupuesto esencial para su ejecución práctica.

Numerosas legislaciones han comenzado a adoptar leyes de transparencia y acceso a la información pública gubernamental, estableciéndose expresamente el derecho a la información y su libre acceso como garantías vinculadas al respeto a la verdad que forjan camino hacia una democracia realmente participativa.

²⁴ HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 63.

CAPÍTULO II.
CONFIGURACIÓN DEL DERECHO A CONTROLAR LOS DATOS PERSONALES
Y HERRAMIENTAS PARA LA PROTECCIÓN DE LOS DERECHOS DE LOS
TITULARES DE DATOS PERSONALES EN EL DERECHO COMPARADO Y
CHILE.

2.1. Las primeras manifestaciones de vulneración de derechos por tratamiento de datos personales y como se concibió que se articulaban en torno a las concepciones de intimidad y *privacy*.

Desde hace varias décadas se ha gestado una creciente preocupación por cautelar los derechos de las personas frente a los progresivos avances tecnológicos y el consecuente desarrollo de técnicas mecánicas y automatizadas de tratamiento de datos, cuyo objeto se centra en la configuración de óptimas segmentaciones para la categorización de personas que permitan tomar decisiones informadas en el flujo de los negocios.

Ahora, si analizamos el bien jurídico que trasciende esta intención normativa podemos visualizar que frente a la posibilidad latente de vulneración de los derechos de los individuos producto del tratamiento de datos personales y el riesgo de cristalizar al ser humano en miles de datos, pensamos en primer término en la intrusión en la intimidad, la vida privada y la dignidad de las personas, concepciones que se gestaron hace decenas de años, mucho antes que pudieran plasmarse en textos legislativos.

Desde tiempos inmemoriales ha existido una propensión del ser humano hacia buscar un espacio propio, apartado de las miradas ajenas. De aquí que progresivamente se haya reivindicado determinados niveles de aislamiento conforme se desarrollan las condiciones sociales y económicas de los seres humanos.

Se comienza a construir la noción de intimidad, la germinación de su idea, su pretensión histórica; y, en un último término su enunciación técnico jurídica, primero

vinculada al derecho de propiedad para posteriormente evolucionar y configurarse como un derecho fundamental autónomo con características propias.

La intimidad aparece en todas las sociedades humanas enlazada al sentimiento de territorialidad como una tendencia humana a someter a su control un espacio físico, ejerciendo sobre él un poder que puede concebirse como una suerte de dominio sobre una “propiedad” en la que podría desarrollarse la intimidad²⁵, comenzando a vislumbrarse la aspiración humana a la protección de este derecho.

Más tarde, en el Derecho Romano se principia a distinguir entre derecho público y derecho privado; y, una identificación del domicilio y la correspondencia con un correlativo de protección determinada. Luego, los siguientes reconocimientos parciales de intimidad vienen dados en el año 313 con el establecimiento del Edicto de Milán y la instauración de la libertad religiosa; y, posteriormente, en la Edad Media traducida en el anhelo germánico por la libertad y la noción cristiana de dignidad de la persona.

Con la Edad Moderna y la Contrarreforma se produjo una separación nítida entre el ámbito religioso y el secular. A partir del momento en que la religión y sus instituciones comienzan a perder influencia sobre la sociedad, la política se transforma. Simultáneamente, se comienza a forjar un reconocimiento de la inviolabilidad del domicilio y el secreto en las comunicaciones.

Si quisiéramos establecer un momento histórico exacto al cual se asocia el nacimiento de la intimidad, cierto sector doctrinal apunta hacia la disgregación de la sociedad feudal y el nacimiento de la sociedad urbana con complejas relaciones sociales y la consecuente modificación en los modos y relaciones de producción. Durante este período la burguesía propietaria puede disfrutar de un ámbito físico propio, cercado a los ojos de terceros extraños, el que se constituye bajo el concepto de domicilio,

²⁵ MARTÍNEZ Martínez, Ricardo, “Una aproximación crítica a la autodeterminación informativa”, Thompson Civitas Ediciones, Madrid, 2004, Pág. 39.

espacio en el que se podrá reivindicar el derecho a ser dejado solo o en paz, es decir, a no ser perturbado por intromisiones sobre las que no se ha consentido.

Tras la Revolución Francesa, comenzó el proceso de positivización de los derechos naturales los que se conceptualizan bajo la forma de derechos subjetivos, cuya finalidad se centró en la idea de otorgar una estrategia técnica capaz de proteger los intereses de los particulares, en especial los referidos a la propiedad. Durante esta época se asocian los conceptos de intimidad con los de propiedad, asimilándose a esta última como condición de la primera en un claro enfoque patrimonialista.

Ya en las obras de autores como Thomas Hobbes, John Locke y Stuart Mill, se profundiza en la noción de intimidad, centrándose en la idea de autonomía para disponer como uno quiera de sus actos, buscando un equilibrio entre la esfera pública y la privada. En los aspectos que conciernen al individuo, éste tiene derecho a una absoluta independencia, siendo soberano de su proceder, reconociendo los límites que podrían trazarse sólo cuando se relacione con otras personas en actos de convivencia.

Sin embargo, el enunciado de un “derecho a la intimidad” como categoría independiente²⁶, orientado hacia la protección de la esfera personal de los individuos, se plasma categóricamente en el artículo de Samuel D. Warren y Louis D. Brandeis en el año 1891. Este artículo buscó establecer la existencia de un límite jurídico que negase las intromisiones de la prensa en la vida privada de las personas.

Con la publicación de este artículo en la *Harvard Law Review* se anticipa el término “*privacy*” como concepto análogo al derecho de intimidad, asumiendo un papel ambivalente; por un lado la intención conservadora, para no proporcionar a los poderes públicos informaciones personales y económicas; y, por otro, desde posiciones progresistas para reaccionar contra la acumulación de datos destinados al control de

²⁶ GILS Carbó, Alejandra, Régimen legal de las bases de datos y hábeas data, Buenos Aires, La Ley, 2001, Pág. 10.

los comportamientos ideológicos con fines discriminatorios²⁷. En este sentido se garantizaría a las personas el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones.

Warren y Brandeis aspiraron a otorgar una solución jurídica a un problema concreto consistente en la determinación de si el *common law* entregaba alguna respuesta frente a las intromisiones en la vida privada de los individuos por parte de la prensa escrita. En aquella época se planteaba un novedoso desafío tecnológico, generado por la fotografía instantánea, que permitía capturar imágenes con prescindencia del consentimiento de las personas, sustrayéndose del control del individuo el destino donde fuera a parar la fotografía.

A través de esta obra, se confecciona un cuerpo teórico que modifica las bases jurídicas sobre las que se venían garantizando determinados derechos de la personalidad, reasentando la tutela concebida en base a la propiedad privada, hacia la protección de la dignidad del hombre y la inviolabilidad de la personalidad humana. “*The Right to Privacy*” publicado en 1890 por Warren y Brandeis concreta el alumbramiento de un nuevo derecho. Sólo hacia 1975 se reconoce constitucionalmente un derecho de estas características en la Constitución Portuguesa.

Lo que caracteriza a la construcción de esta nueva realidad se define en términos de la facultad del individuo de ejercer determinado control sobre su vida privada traducido en la facultad de decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones²⁸.

Ya en esta etapa inicial de desarrollo del derecho a la intimidad y a la privacidad, se entiende que estos no son derechos ilimitados. En efecto, no se impedirá la publicación

²⁷ CASTILLO Jiménez, Cinta, Las nuevas tecnologías de la información y el derecho de Vittorio Frosini a Internet, Instituto de Estadística de Andalucía, Consejería de Economía y Hacienda, Sevilla, 2003, pág. 87.

²⁸ WARREN, S. D. y Brandeis L. D.: “The right to privacy”, en Harvard Law Review, vol. IV, núm. 5, diciembre de 1890, Pág. 31.

de aquello que arraigue un interés público o general, siendo relevante además la condición pública o privada que detenta el individuo, lo que no quiere decir que los hombres públicos no tiene derecho a ver protegida parte de su vida privada, sino que obviamente su vida se lleva de manera más expuesta y este aspecto debe tenerse en cuenta. Asimismo, el derecho a la intimidad y a la vida privada decae cuando la publicación de los hechos ha sido realizada por el mismo individuo o con la intervención de su consentimiento.

Desde sus orígenes, la *privacy* norteamericana ha gozado de una textura abierta, dotándose de la capacidad de atender a las repercusiones que se vayan suscitando a través del avance científico y tecnológico mantenido en el tiempo. Este fenómeno es posible por el sistema jurídico norteamericano. En efecto, la Constitución Norteamericana no contiene una lista cerrada de derechos sino que se establece, a través de la Novena Enmienda, una cláusula de apertura a la incorporación de nuevos derechos²⁹.

No puede desconocerse la gran influencia de la doctrina norteamericana y la jurisprudencia del Tribunal Supremo de los Estados Unidos, pero debemos tener en cuenta que las conclusiones que se plasman en este país provienen de un modelo jurídico diametralmente distinto al derecho continental.

Cuando hablamos de la noción de *privacy* conceptualizada en el artículo de estos autores norteamericanos, debemos distinguir que este concepto ha pretendido abarcar una extensión mayor que la que empleamos para referirnos a la intimidad. La intimidad estaría más restringida y limitada a los aspectos más internos del individuo, mientras que la *privacy* abarca una esfera más amplia que puede integrar, simultáneamente, a

²⁹ En el sistema jurídico del *common law*, el término *privacy* es excepcionalmente amplio, de manera que es bastante difícil determinar con precisión el contenido de su significado. En su evolución la *privacy* se extendió paulatinamente, hasta llegar a incluir desde aspectos de tipo penal hasta decisiones de tipo personal asociadas al área reproductiva o de índole sexual. Entre estos dos extremos, se comprende, asimismo la protección de la honra de la imagen, de la inviolabilidad del hogar, de las comunicaciones, entre otras temáticas.

los aspectos más íntimos, aquello que el propio individuo quiere mantener en su esfera más privada.

En efecto, mucho se ha dicho acerca de la distinción entre privacidad e intimidad, en especial en lo referente a que lo íntimo, es más privado aún que lo privado. El fuero íntimo de una persona es lo que sólo le pertenece a ella y está exento de cualquier objetivación forzosa³⁰. De aquí que algunas legislaciones hayan optado por utilizar en sus Cartas Fundamentales el término de privacidad o vida privada en vez de optar por el término intimidad, de manera de poder ampliar el espectro de protección, entendiendo que la vida privada no se agota en lo “meramente privado” sino que tiene una faceta social ineludible, es decir, que contempla la interrelación social del ser humano.

Sin embargo, pese al acento que ha empleado la doctrina para resaltar que intimidad y privacidad son dos conceptos distintos, ambos términos se usan de manera indistinta en la cotidianidad, llegando algunos autores a señalar que ni lingüística ni jurídicamente hablando, habría diferencias sustanciales, ya que ambos hacen referencia a determinado aspecto reservado donde sólo tienen acceso determinadas personas.

Incluso el Tribunal Constitucional español ha llegado a invertir la relación intimidad – privacidad, señalando que “el derecho constitucional a la intimidad excluye las intromisiones de los demás en la esfera de la vida privada personal y familiar de los ciudadanos³¹”, lo que trae consigo la reconducción mutua de los conceptos.

La presencia de una nueva realidad tecnológica no obsta a la aplicación de principios jurídicos preexistentes debidamente ajustados al nuevo contexto. Se debe reconocer,

³⁰ BIANCHI, Alberto, Hábeas Data y Derecho a la privacidad, en Revista Jurídica El Derecho, tomo 160 – 866, Buenos Aires, Argentina.

³¹ RUIZ, Miguel Carlos, La configuración constitucional del derecho a la intimidad, Madrid, Tecnos, 1995, Pág. 29

por lo tanto, que tanto la intimidad como la privacidad son un soporte y presupuesto de otros derechos, como la libertad y el libre desenvolvimiento de la personalidad.

Transcurridos más de cien años desde la primera formulación del concepto de privacidad e intimidad, la enunciación de estos derechos ha adquirido un nuevo significado, incorporando la idea de que cuando hablamos de intimidad no sólo hacemos referencia a las relaciones entre los individuos particulares, sino también a las relaciones entre el individuo y terceros como la administración pública u otros órganos desarrollados.

Ahora, cabe preguntarse si la intimidad y la privacidad son conceptos aptos para alzarse como bienes jurídicos a tutelar a través de la protección de los datos personales frente a su tratamiento automatizado. Los obstáculos más importantes que encontramos a la hora de decidir si estos derechos alcanzan el contenido que necesitamos resguardar se centran en la dificultad de precisar sus alcances y las facultades que ambos otorgan.

En cuanto a la dificultad de precisar sus alcances nos referimos que al hablar de intimidad y privacidad es inevitable que lleguemos a la concepción de un término dotado de gran contenido emocional y sometido a variados cambios motivados por las circunstancias sociales del momento histórico, en especial aquello que se considera más subjetivo para el individuo. De aquí que no exista un acuerdo unánime sobre lo que podemos llamar intimidad, sino solamente intentos doctrinales, legales y jurisprudenciales de definición que han conducido a un alto de grado de indeterminación y equivocidad que dificulta precisar su contenido y alcance jurídico. Parece ser tributo inevitable de los conceptos y categorías más recurrentes en la teoría jurídica adolecer de un déficit de intención conceptual proporcionalmente inverso a la extensión de su uso³².

³² PÉREZ Luño, A. E., Dilemas actuales de la protección a la intimidad, en Dilemas actuales de los derechos fundamentales, Universidad Carlos III – Boletín Oficial del Estado, Madrid, 1994, pág. 313.

En tanto, cuando nos preguntamos sobre las facultades que podemos desplegar al considerar que nuestro derecho a la intimidad o a la privacidad ha sido vulnerado, encontramos las limitaciones que la doctrina ha considerado más importantes, y que se refieren a que estos derechos no otorgan una facultad de control clara, en orden a conocer quién, por qué y cómo ha obtenido nuestra información personal, ya que sólo se centra en el significado negativo de la defensa ante la intervención ajena.

El siguiente obstáculo dice relación con que frente al tratamiento de datos personales puede suceder que los derechos vulnerados no sean solamente los derechos de intimidad o privacidad, sino que la contravención abarque otros derechos distintos, como el derecho a la vida, a la salud, al trabajo, etc.

Es así, como frente a las nuevas tecnologías de la información se ha suscitado la difícil discusión sobre la posibilidad de construir conceptual y jurídicamente un nuevo derecho fundamental que resguarde a la persona frente a la recogida, tratamiento y manejo de la información que le concierne, recogiendo los aspectos más relevantes que los conceptos de privacidad, intimidad, honra, etc. han aportado a esta experiencia. O si bien, dar un paso de esta magnitud no es necesario y a través de la ampliación del derecho a la intimidad y la privacidad podemos otorgar a los individuos las defensas necesarias ante los avances tecnológicos que trae consigo la sociedad de la información.

2.2. Mutación de la concepción de intimidad y *privacy* hacia el reconocimiento de un nuevo derecho llamado autodeterminación informativa y libertad informática.

En este contexto, cuando el progreso técnico crea nuevas amenazas al bienestar de los individuos, nace o se adapta un derecho fundamental correlativo que en su existencia materialice una protección adecuada. Esta redefinición o incorporación del nuevo derecho, tiene por objetivo plasmar en el ordenamiento jurídico una protección capaz de hacer frente a las nuevas realidades que amenazan a los seres humanos.

Precisamente, los problemas conceptuales que arraigan la intimidad y la privacidad, han motivado la búsqueda de una alternativa capaz de suplir estas debilidades. Si bien el problema aún suscita controversia entre las diferentes esferas del derecho, ya hacia 1983 el Tribunal Constitucional Alemán comenzaba a postular la existencia de un derecho paralelo y autónomo al de intimidad o privacidad, centrado en la facultad de toda persona para desplegar determinado control sobre la información personal, contenida en registros públicos o privados, especialmente los datos acopiados en registros informáticos.

El 15 de diciembre de 1983 el Tribunal Constitucional Federal Alemán resolvió el recurso interpuesto contra la Ley de Censo de Población, declarándola inconstitucional, en razón del excesivo número de datos e informaciones solicitadas a los ciudadanos con la finalidad de ser sometidas a un posterior tratamiento informatizado.

Como habíamos adelantado, la Ley del Censo de la Población fue publicada en marzo del año 1982 y durante toda su tramitación pasó casi inadvertida ante la población, sin embargo, al ponerse en vigor produjo una protesta sin precedentes en el territorio de Alemania. Se pretendía requerirles a los individuos datos sobre sus nombres, apellidos, dirección, teléfono, sexo, fecha de nacimiento, ideología política, religión, nacionalidad, tipo de convivencia con otras personas, domicilio, clase de trabajo, ingresos, profesión, duración de los estudios, dirección laboral, medios de locomoción utilizados para desplazarse, tiempo promedio empleado para realizar el recorrido, duración de la jornada de trabajo, clase, extensión, dotación y uso de la vivienda, número y uso de las habitaciones, cuantía de los dividendos o arriendos mensuales. El ciudadano percibió con recelo esta gigantesca operación de censo en que se exigía a las personas una información personal exhaustiva, planteándose la posibilidad de que el gobierno quisiera tomar control sobre las actividades de los individuos y las condiciones personales de los ciudadanos.

El Tribunal Constitucional Federal Alemán estableció líneas directrices que sentaron las bases para la configuración de este derecho llamado autodeterminación informativa, partiendo de la premisa que se garantiza al individuo la facultad de

determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona, admitiéndose limitaciones a este derecho sólo en la medida que ceda ante un interés general superior.

Sería incompatible con el orden social y jurídico la posibilidad de que un individuo no sea capaz de discernir que informaciones relativas a él son conocidas en diversos sectores de su entorno social, sustrayéndosele la facultad de verificar la información que está siendo conocida de él. Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda capacidad de obrar y de cooperación de sus ciudadanos³³.

De aquí que sea esencial otorgar a las personas autonomía sobre su consentimiento en cuanto a la posibilidad de autorizar, bloquear, oponerse, rectificar la información que está circulando a su respecto, configurándose la autodeterminación informativa como la facultad del individuo de decidir básicamente por sí mismo cuando y dentro de qué límites³⁴ procederá a revelar situaciones concernientes a su vida privada.

Desde este punto se inicia el debate doctrinal acerca de si la autodeterminación informativa es un nuevo derecho fundamental o si se trata de una ampliación del derecho general de la personalidad. Es decir, o consideramos que la autodeterminación informativa es un derecho autónomo e independiente, o bien, la concebimos como un elemento encuadrado dentro de los derechos generales de la personalidad y asociado a los conceptos de intimidad, vida privada, honra y dignidad, ampliamente reconocidos en las cartas fundamentales nacionales.

³³ Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán. Considerando C. II. I., Boletín de Jurisprudencia Constitucional, IV Jurisprudencia Constitucional Extranjera, Pág. 153.

³⁴ ÁLVAREZ González, Susana, Derechos fundamentales y protección de datos genéticos, 1º Edición, Instituto de Derechos Humanos Bartolomé de las Casas, Universidad Carlos III de Madrid, 2007, Pág. 78.

Afirmar la existencia de un derecho a la autodeterminación informativa implica la consideración de un derecho con un objeto y un contenido distinto a los derechos de intimidad y privacidad, con un ámbito más amplio y elementos más complejos, abarcando el elemento negativo de exclusión del conocimiento ajeno de cuanto hace referencia a la persona, típico aspecto del derecho a la intimidad y a la privacidad, y el elemento positivo consistente en la facultad de control por el sujeto de los datos personales relativos al círculo íntimo, esto es, la disposición de un poder de control sobre la publicidad de las informaciones³⁵.

También la doctrina española ha hecho eco de este debate, haciéndose presentes las mismas dos posturas, pero denominando a este derecho de control sobre la información personal: libertad informática. A través de la sentencia del Tribunal Supremo español, 254/1993, de fecha 20 de julio se profundiza sobre el alcance del artículo 18 de la Constitución que en sus apartados uno a cuatro garantizan el derecho al honor, a la intimidad personal y familiar y a la propia imagen, estableciéndose en el apartado final que “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”.

El problema desarrollado a través de esta sentencia, dice relación con la petición del recurrente de amparo, en cuanto a solicitar información acerca de los ficheros automatizados donde figurasen datos de carácter personal que le concernían, la finalidad de estos y su respectiva comunicación. Ninguna de las autoridades a las que se dirigió, dictó resolución respecto a sus peticiones, arguyéndose en la defensa la falta de invocación del derecho fundamental en la vía judicial previa y la imposibilidad material en que se encontraban las autoridades para contestar las peticiones del recurrente, defensas que se desestimaron.

El tribunal determinó que la cuestión a discernir era si el recurrente tenía o no derecho, en virtud del artículo 18.4 de la Constitución, a que la administración le suministrara la

³⁵ ÁLVAREZ González, Susana, Derechos fundamentales y protección de datos genéticos, 1º Edición, Instituto de Derechos Humanos Bartolomé de las Casas, Universidad Carlos III de Madrid, 2007, Pág. 89.

información solicitada, entendiéndose que si tenía derecho, era deber de todos los poderes públicos poner los medios organizativos y materiales necesarios para procurar su provisión.

Las peticiones de información formuladas en el recurso, se fundaban en el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984, resultando esencial para la resolución favorable del recurso, el reconocimiento de este Convenio en su efecto directo o interpretativo.

La sentencia adopta efectivamente esta tesis, es decir, considera que pese a la ausencia de desarrollo legislativo constitucional de las garantías esgrimidas por el recurrente, debe reconocerse que los derechos a obtener información, ejercitados por el demandante de amparo, forman parte del contenido mínimo que consagra el artículo 18.4 de la Constitución.

De esta forma, el contenido básico de las garantías contempladas en el artículo 18.4 de la Constitución se complementa a través de los elementos negativos y positivos que le son propios. Tenemos por un lado, que el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y el pleno ejercicio de sus derechos; y, por el otro, un contenido positivo que forma parte del derecho de control sobre los datos relativos a la propia persona, llamada libertad informática como derecho a controlar el uso de los mismos datos insertos en un programa informático.

Desde esta óptica las legislaciones de diferentes países han optado por acoger un derecho denominado hábeas data, que se comporta simultáneamente como una garantía procesal para tutelar el bien jurídico y como un derecho específico surgido de la información automatizada, por medio de la cual cada individuo tiene derecho a controlar las informaciones que sobre su persona constan en bancos de datos, o en

redes mundiales de información³⁶, adoptando el elemento positivo que otorga la autodeterminación informativa y la libertad informática.

Por lo tanto, cuando el hábeas data se materializa como un mecanismo procesal, opera como una herramienta procesal para la defensa de otros derechos fundamentales como la intimidad, la privacidad, el honor, la dignidad humana, la propiedad, etc.

Como señala Rafael Ortiz, el derecho de hábeas data consiste en el reconocimiento por parte de los ordenamientos jurídicos de los pueblos de la posibilidad de control de la información automatizada que sobre personas o grupos (comunidades) puede encontrarse en manos del Estado o de particulares; este derecho de control implica: acceso, control de la finalidad y el uso, rectificación y destrucción cuando sea adversa.

El énfasis de la propuesta está en la proclamación del derecho de auto tutela de la propia identidad personal que facultará al individuo a conocer y acceder a las informaciones que le conciernen y que constan en un banco de datos, de manera de controlar su calidad y ejerciendo el derecho a corregir, modificar o cancelar aquella información indebidamente procesada.

En este punto podemos ver con claridad la insuficiencia que reside en los conceptos de intimidad o privacidad para centrarse como bienes jurídicos rectores de la protección de datos personales. Aquello que realmente permite al individuo no resultar vulnerado a través del tratamiento de datos personales es la existencia de una facultad a conocer y examinar las informaciones personales. Por esta razón se debe afirmar que todos los datos personales deben ser protegidos, indiferentemente del interés que tenga la sociedad en ellos. Un dato no tiene que ser necesariamente íntimo para que detente una tutela legal, lo que se protege es la facultad de individuo de decidir sobre este aspecto.

³⁶ ORTÍZ Ortiz, Rafael, Hábeas data: derecho fundamental y garantía de protección de los derechos de la personalidad, Caracas, 2001, Pág. 236.

Los derechos de autodeterminación informativa y libertad informática, materializados en su facultad de control, se constituyen como presupuestos necesarios para el funcionamiento de los actuales sistemas democráticos al impulsar individuos libres e iguales. Como advierte Vittorio Frosini, la nueva fórmula sustituye el antiguo “*right to privacy*” que se concentra en el significado negativo de defensa ante la intervención ajena, agregando el significado positivo. Ello consiste no sólo en la afirmación de una esfera de privacidad, sino también en la facultad de acceso, control, de rectificación y de cancelación de los datos personales insertos en un banco de datos³⁷.

2.3. Aceptación de la autodeterminación informativa y la libertad informática como derechos de control de datos personales.

El concepto de hábeas data tiene su origen etimológico en la expresión *hábeas corpus*, el que nació como una institución jurídica creada para garantizar la libertad personal del individuo, con el objetivo de evitar los arrestos y detenciones arbitrarias. Este término se origina del latín *habeās corpus [ad subiiciendum]* que tengas [tu] cuerpo [para exponer]’, “tendrás tu cuerpo libre”, proclamando determinado control sobre el cuerpo del individuo, sobre su libertad física.

El hábeas data se refiere a esta misma facultad de control pero no respecto a la libertad del cuerpo, a lo corporal o ambulatorio, sino a la libertad del individuo de conocer, mostrar o exhibir el dato³⁸, esto es, la información que le concierne y que consta en un registro material de datos, ejerciéndose un control relativo a la existencia misma de los datos, la finalidad con que han sido recogidos y el uso que se les ha dado.

³⁷ FROSINI, Vittorio, La tutela de la privacidad de la libertad informática al bien jurídico informático, Revista de Colegio de Abogados, Buenos Aires, 1989, Pág. 96.

³⁸ ORTÍZ Ortiz, Rafael, Hábeas data: derecho fundamental y garantía de protección de los derechos de la personalidad, Caracas, 2001, Pág. 237.

De esta facultad de control se desprende la posibilidad de que el titular de los datos personales pueda completar, rectificar, actualizar, proteger e incluso destruir aquellos datos que provoquen un potencial daño al individuo en sus derechos fundamentales, concretándose como una auto tutela de su propia identidad.

El acento que se pone en la serie de derechos pertenecientes al titular de la información tiene por objeto preservar las facultades del individuo no sólo en relación a los datos íntimos que le pertenecen, sino también en cuanto a los datos que no son necesariamente íntimos. Como advierte Pablo Lucas Murillo, por ejemplo, que tiene de íntimo y de secreto el hecho de que una persona tenga una tarjeta de crédito, que tenga determinado vehículo o que sea cliente de determinadas empresas, y qué interés podría haber de tutelar estos aspectos como áreas específicas de la reserva del ser humano³⁹.

Señalamos anteriormente que los conceptos de intimidad y privacidad son insuficientes en el contexto del tratamiento automatizado de datos personales. Hoy en día se pueden vulnerar aquellos ámbitos que el individuo acostumbraba exteriorizar producto del ejercicio de otras esferas de su personalidad que redundan en un “estado intermedio entre lo privado y lo público⁴⁰”, pero que sin embargo, aún alcanzan a la personalidad del ciudadano que hace uso de su libertad para definir su proyecto de vida.

Como hemos señalado en el primer capítulo, en estas hipótesis se percibe la necesidad de tutela, extendida al control del individuo respecto a todos los datos, pues estamos ante áreas de convivencia en las que una interconexión de datos aislados que en sí mismos no poseen un interés relevante, unidos, generan la posibilidad de

³⁹ LUCAS MURILLO DE LA CUEVA, Pablo, Informática y Protección de Datos Personales, Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, Madrid, Centro de Estudios Constitucionales, 1993, Pág.30.

⁴⁰ HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 113.

establecer un perfil bastante aproximado o quizás incluso exacto de la persona, sus características, sus gustos, su comportamiento.

Por lo tanto, la esencia del concepto de control de los datos personales radica en las facultades que se le otorgan al individuo para hacer frente a los riesgos que arraiga el tratamiento automatizado de datos personales y la necesidad de afianzar el rol del ciudadano en una democracia que ha adquirido nuevas características particulares, trazadas por el papel relevante que ha adquirido la circulación de información.

Lo fundamental será entonces el derecho del individuo a saber cuáles datos de su titularidad están siendo tratados, con qué finalidad están siendo manipulados, cuáles son las personas implicadas en el proceso de tratamiento y bajo qué circunstancias se están realizando dichas intervenciones. En este sentido, el derecho a controlar los datos personales, debe sustentarse en los siguientes principios que conducirán su conceptualización:

- El principio de libertad de decisión del titular de los datos sobre la finalidad y el objetivo del procesamiento de datos personales es la fiel manifestación de que el dueño de los datos personales es el titular de los mismos. El banco de datos no se convierte en el propietario de los datos por el sólo hecho de haberlos recolectado, de manera que el titular de los datos tiene libre disposición de los mismos, requiriéndose del consentimiento del afectado para que éstos puedan ser tratados.

- El principio de transparencia sobre el tipo, dimensión y fines del procesamiento de datos. En todo proceso de tratamiento de datos personales, los datos deben ser recogidos para fines determinados y legítimos, y no deben ser utilizados de manera incompatible con tales fines delineados. Con antelación al inicio del tratamiento de datos personales debe manifestarse la finalidad que arraiga el procedimiento, pues sólo así se podrá comprobar si los datos están siendo utilizados de acuerdo a la finalidad para la que fueron recogidos, estableciéndose la distinción entre cuales son los datos adecuados, pertinentes y no excesivos respecto a los objetivos para los que fueron recogidos, en un aspecto cualitativo y cuantitativo.

- El principio de división técnica y organizacional entre el procesamiento de datos frente a otros fines de utilización de los datos personales (principio de separación de poderes informativos). Los bancos de datos contienen datos de determinadas categoría, por ejemplo, datos provenientes del área de la salud, no deben terminar en registros utilizados para fines laborales.

- El principio de prohibición del procesamiento de datos “a beneficio de inventario” o para acopiarlos con el fin de simplificar la realización de un ulterior tratamiento de datos no autorizado por el titular de la información. Los datos deben ser conservados de tal forma y durante un período de tiempo tal que sólo permita identificar a los afectados durante el plazo que sea necesario para conseguir los fines para los que fueron recogidos. En definitiva, debe reconocerse aquello que se ha denominado como “derecho al olvido” mediante la implementación de reglas de destrucción de los datos personales una vez que ha sido cumplido el fin para que fueron recopilados.

- Principio de calidad de los datos. Los datos recogidos y almacenados deben ser exactos y actuales, es decir, deben irse poniendo al día, evitando los perjuicios que podrían provocarse al titular de los datos por la existencia de errores o datos no fiables.

Estos principios que fundamentan el concepto de autodeterminación informativa y libertad informática, capaz de sustentar un adecuado sistema de protección de datos personales, conllevan varios derechos derivados del control que tiene el individuo sobre su propia información personal como antecedentes configuradores de su proyecto de vida:

- i. Derecho a ser informado del tratamiento de datos personales: esta facultad es el derecho por antonomasia que sustenta el concepto de autodeterminación informativa. Mediante éste, el titular de los datos personales tiene derecho a ser informado acerca de diversos puntos, entre los que se encuentran los siguientes más relevantes:
 - La existencia de un banco de datos en que constan sus datos personales.

- La procedencia de los datos recogidos y organizados en el banco o fichero de datos personales.
- El propósito del almacenamiento de datos personales.
- Las personas u organismos a los que se ha comunicado sus datos personales.

Sólo a través de este derecho, el titular de los datos estará en posición de ejercer un control adecuado de la información que está siendo tratada, conociendo los datos erróneos, inexactos, equívocos, incompletos o caducos, posibilitándose su defensa frente a las vulneraciones a su derecho.

ii. Derecho a consentir en el tratamiento de datos personales: esta facultad está bastante ligada a la anterior, pues sólo en el supuesto que se haya informado sobre la existencia de un proceso de tratamiento de datos personales y su contenido, el titular está en posición de consentir.

Este derecho es el reconocimiento correlativo del derecho a la libre disposición de los datos personales, esencia de la protección de datos, que se traduce en la necesidad del consentimiento del titular de los datos para que éstos puedan ser tratados.

Como señala Ana Herrán sólo a partir del reconocimiento del principio de consentimiento informado en el tratamiento de datos personales, se permite la estructuración y organización de la autodeterminación informativa o la facultad de los interesados de establecer y decidir sobre el tratamiento de información que le concierne⁴¹.

iii. Derecho de acceso a los datos que están siendo objeto de tratamiento de datos personales: el derecho de acceso es una de las manifestaciones del reconocimiento del derecho a ser informado. Se traduce en el precepto de que cada individuo debe

⁴¹ HERRÁN Ortiz, Ana Isabel, El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales, Madrid, Editorial Dykinson, 2002, Pág. 220.

tener la facultad cierta de saber qué datos suyos han sido recogidos, almacenados o tratados en ficheros o archivos que contengan datos personales suyos.

iv. Derecho de modificación, eliminación, bloqueo y cancelación: estos derechos también nacen bajo el presupuesto que el titular del banco de datos haya informado al afectado, sobre qué datos están siendo tratados.

a. Derecho a la modificación de los datos personales: cuando los datos sean erróneos, inexactos, equívocos o incompletos.

b. Derecho a la eliminación de los datos personales: cuando el almacenamiento de los datos carezca de fundamento legal o cuando los datos estuvieren caducos.

c. Derecho a bloquear los datos personales: esto ocurre en el caso que el titular de los datos personales no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

2.4. Herramientas para la protección de los derechos de los titulares de los datos personales: el derecho a ser informado en sus distintas modalidades.

Una de las mayores limitaciones a la tutela de los datos personales, paralela a los problemas conceptuales que ya hemos recorrido, dice relación con una de las características fundamentales que arraigan los avances tecnológicos en la actualidad. La protección de los datos personales no puede partir de la premisa de que será el individuo quien se dé cuenta de la lesión que podrá producirse producto del tratamiento de datos personales, sea de parte del Estado o de un particular.

La conceptualización de un hábeas data no puede estar estructurada de manera que sea el individuo quien ha de ofrecer las pruebas que fundamenten aquel hecho u omisión que se le imputa a determinado órgano titular del banco de datos. Estos requisitos que resultan obvios ante el planteamiento de recursos judiciales y que tienen

sentido dentro del contexto de las lesiones a derechos fundamentales⁴², en materia de protección de datos personales resultan utópicos e impracticables.

El tratamiento de datos personales no es sólo un proceso bastante inaprensible y poco agresivo frente a los ojos de los individuos afectados, es incluso una herramienta tecnológica tentadora y deseada, pues los riesgos eventuales que pueden provocarse son disimulados tras los beneficios que se logran, esgrimiéndose promesas de seguridad, eficiencia, velocidad y disminución de los obstáculos propios de la burocracia.

Tras este edén tecnológico se encubre la realidad de que hoy el procesamiento de datos personales tiene una movilidad inusitada y descentralizada, cuyos contornos son difíciles de dimensionar. La interconexión de los registros de datos, el rol del Estado como un observador – colaborador, la persona u órganos que realizan silenciosamente las lesiones, son imperceptibles, enmascarándose tras los procesos técnicos automatizados cuyas características les permiten vivir en la clandestinidad.

En este contexto es que la evolución del derecho a la autodeterminación informativa o libertad informática, reflejada en la facultad de controlar los datos personales, debe llevar hacia una nueva estructuración de la forma de tutela que ofrecen estos derechos, orientados hacia una concepción más preventiva que reactiva, emplazada hacia la beneficiosa potencialidad que detentan los derechos de información al individuo, viabilizando un control técnico constante del tratamiento de datos personales que otorgue certeza a los ciudadanos que el procesamiento de sus datos personales se realizará dentro de un marco de efectiva legalidad.

Ya hemos señalado la importancia que se le atribuye hoy a la información. En este sentido, para los bancos de datos la información es un recurso valioso a la hora de tomar decisiones en el mercado. Para los particulares, en tanto, la información que les

⁴² HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, Pág. 148.

concierno es imprescindible en su propio desarrollo y el conocer aquellos datos personales que constan en registros tecnológicos aporta importantes elementos para que éste pueda orientar su actuar.

El derecho a ser informado constituye una instancia necesaria e indispensable para la participación ciudadana y la protección de los derechos correspondientes. Sin información adecuada, oportuna y veraz, los individuos están imposibilitados de participar en la sociedad en condiciones óptimas y consecuentes con un Estado democrático.

Precisamente por esta misma razón, se ha desarrollado la necesidad de utilizar la información de forma racional y productiva, en beneficio del ser humano y la comunidad, y no de manera inversa. Para el cumplimiento de este fin, las Cartas Fundamentales de diversas naciones han establecido derechos de información como garantías individuales de toda persona, fomentando la creación de Leyes de Transparencia y Acceso a la Información Pública Gubernamental como reflejos últimos del respeto a la verdad, al rechazo a la corrupción y al incremento de la transparencia en los sistemas democráticos.

Este derecho del individuo de estar veraz y objetivamente informado con respecto al actuar del Estado, se intensifica si se trata de su misma información. Aquí no hablamos del actuar de terceros, de cómo otros han procedido, sino por el contrario, de aquello que concierne precisamente al círculo más próximo al ser humano, su propia vida e individualidad.

Es así trascendental que el Estado asuma la obligación de procurar que la actividad de tratar información del propio individuo, en manos de terceros, sea una labor ejecutada de forma transparente. No es el ser humano el que deba adquirir una calidad de cristal frente al procesamiento de sus datos personales, sino que es el registro de datos el que debe cristalizarse para que todo ciudadano que así lo requiera, pueda recibir en forma práctica y expedita, conocimientos en la materia o asunto que sea de su interés.

El establecimiento de la obligación de entregar información veraz, la instauración de plazos específicos para su entrega, la creación de vías administrativas y judiciales adecuadas para proceder frente a la denegatoria o entrega parcial de la información solicitada, la imposición de sanciones y el régimen de excepciones, son sólo algunos de los aspectos sustanciales que deben ser contemplados en las legislaciones de protección de datos personales, que permitirán, en definitiva, poner a disposición de la comunidad el desarrollo individual y colectivo de los individuos.

En este sentido se hace vital que el ordenamiento interno de los países reconozca la existencia del derecho de autodeterminación informativa o libertad informática como un derecho fundamental con un contenido jurídico que estaría formado por las diferentes herramientas que integran la protección de datos personales y que posee un núcleo o reducto indisponible incluso para el legislador⁴³, constituyéndose por aquellas facultades necesarias e indispensables para otorgar efectividad a la tutela de todos los derechos que pueden ser vulnerados y que se materializan en las facultades de control que deben desplegarse en función del titular de los datos.

Deben reconocerse nítidamente los elementos negativos y positivos que configuran la autodeterminación informativa. En los primeros se encontrarán aquellas facultades tendientes a la limitación de la utilización de las herramientas tecnológicas como los principios de calidad de los datos, pertinencia, finalidad, veracidad, exactitud, lealtad y seguridad. En tanto, el elemento positivo se concreta en el abanico de facultades que garantizan al individuo el conocimiento sobre quién, qué, cuándo y con qué motivo puede conocer los datos que le conciernen⁴⁴, facultades que se materializan en la forma de la acción de hábeas data que otorga al titular de los datos un conjunto de derechos que puede ejercer frente a quienes son titulares de los bancos de datos con la finalidad de conocer la existencia de tales registros de datos personales, el contenido que los conforma, el uso y el destino que se les contempla.

⁴³ LUCAS MURILLO DE LA CUEVA, Pablo, La construcción de derecho a la autodeterminación informativa, Revista de estudios políticos, ISSN 0048-7694, N° 104, 1999, Madrid, España, Pág. 39.

⁴⁴ PÉREZ LUÑO, A.E.: Comentario legislativo: La LOARTAD y los derechos fundamentales, Madrid, Pág. 407.

La extensión del derecho a ser informado debe ser amplia, de manera de impulsar la transparencia definitiva de los bancos de datos. En este sentido, es de fundamental importancia que contemple:

- El derecho a ser informado sobre la existencia del banco de datos. Este es el punto de partida para todo el entramado de derechos que se promueve a través del derecho a controlar los datos personales pues como señalamos no se puede pretender que la protección se realice cuando los derechos ya han sido vulnerados, es decir reactivamente. Un adecuado sistema de protección de datos personales procurara una defensa preventiva, lo que va más acorde con la naturaleza de los bancos de datos, los que tienen un carácter poco transparente, de manera que lo más probable es que el tratamiento se realice a espaldas de los afectados, prescindiendo de su total conocimiento.
- El derecho a ser informado sobre el contenido del banco de datos. Una vez que el titular de los datos ha sido informado sobre la existencia de un fichero en el que constan datos que le conciernen, debe concedérsele el derecho a acceder al contenido que conforma el registro, es decir, cuáles son los datos exactos que están siendo tratados, de manera de verificar si su tratamiento es procedente y si se trata de información cierta y veraz.
- El derecho a ser informado sobre la finalidad del banco de datos. Toda recogida de datos personales tiene que tener un fundamento y un objeto determinado para justificar la creación del banco de datos. Esta finalidad debe ser determinada en el sentido de tener una magnitud claramente delimitada, de manera de tratar sólo aquellos datos que sean adecuados, pertinentes y no excesivos en proporción a los fines que han sido recogidos, cualitativa y cuantitativamente.
- El derecho a ser informado sobre la procedencia de los datos. Cuando los datos no han sido recogidos directamente del afectado, éste tiene derecho a que se le informe sobre la fuente de la que han sido obtenidos los datos personales.

- El derecho a ser informado sobre el carácter forzoso o voluntario de las respuestas y el propósito para el que se está solicitando la información. Cuando se trate de datos personales recogidos a través de recolecciones mediante encuestas, estudios de mercado o sondeo de opinión pública u otros instrumentos similares, se deberá informar al titular de los bancos de datos sobre el carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. En este sentido, muchas personas responden interrogantes planteadas en estos formatos, asumiendo que se trata de información que figurará anónimamente.
- El derecho a ser informado al solicitar el consentimiento del afectado. En la hipótesis que el banco de datos pretenda solicitar el consentimiento de determinado individuo, deberá previamente dar cabal cumplimiento al deber de información, de manera de posibilitar que la persona entregue un consentimiento informado, libre de vicios.
- El derecho a ser informado cuando se efectúe transmisión de datos. Cuando los datos han sido comunicados a personas determinadas o determinables, el responsable del registro de datos debe informar con la mayor brevedad posible sobre este hecho, individualizando a las personas y organismos a los que se les ha transmitido dicha información.
- El derecho a ser informado sobre las facultades de modificación, eliminación y bloqueo de datos cuándo corresponda y cómo pueden ejercerse.

Un sistema jurídico íntegro, deberá velar porque las disposiciones relativas a las diversas modalidades en que se refleja el derecho a ser informado sean efectivamente observadas por los diferentes actores que intervienen en el tratamiento de datos personales y, muy especialmente, por los titulares y responsables de los bancos de datos, sea que éstos recojan los datos a través de los mismos titulares o mediante terceros. Si no se contemplan mecanismos precisos y efectivos para cumplir estos fines, la consagración en la ley no será suficiente para cumplir la protección de datos personales.

Se requiere un órgano con competencia específica para promover la protección de datos personales, encargado de fiscalizar el cumplimiento de la obligación de informar, quien deberá seguir de cerca cómo se desarrolla el procesamiento de datos personales en ambos extremos de la relación, es decir, como ejecuta el titular del banco de datos sus obligaciones en el tratamiento de datos personales y como se desarrollan las garantías para el titular de los datos personales.

Es preciso, que se avance más allá de la promulgación del derecho a ser informado, materializando en la práctica cuáles son las hipótesis en que se ha cumplido el deber de información y en cuáles se ha incumplido, tarea que se verificará regulando los siguientes puntos:

- Cómo se desarrolla la obligación que asiste al titular de los datos personales de informar ampliamente al afectado cuando los datos han sido recogidos del titular y cuando se han obtenidos de un tercero.
- Modalidad del derecho a ser informado (de oficio o a petición de parte). La ley de protección de datos personales debe especificar cómo se cumple la obligación de informar, es decir, si debe procederse a solicitud del afectado o de oficio, priorizando la información de oficio, por las características del tratamiento de datos personales que como ya mencionamos suele desarrollarse con total desconocimiento del titular de los datos y encubierta por sus atractivos beneficios tecnológicos.
- Establecimiento de plazos específicos para la entrega de la información. No puede entregarse absoluta discreción al titular del banco de datos para que sea el quién decida cuando procede a dar cumplimiento a la obligación de informar
- Creación de vías administrativas y judiciales adecuadas para proceder frente a la denegatoria o entrega parcial de la información solicitada. Aquí debe otorgarse al afectado un recurso apto para funcionar de manera preventiva, evitando futuras lesiones en sus derechos fundamentales, que entregue soluciones expeditas, simples y

eficientes, en manos del órgano fiscalizador y en una segunda instancia en manos de los tribunales de justicia.

- Imposición de sanciones. Para que la legislación de protección de datos personales sea autosuficiente debe establecerse un régimen de sanciones que disuada al titular del banco de datos de incumplir el deber de información, de manera que ante las consecuencias, éste prefiera optar por dar cumplimiento cabal a la obligación que le asiste.

- Régimen de excepciones. Debe reconocerse que existen ciertas materias donde el derecho a ser informado se encuentra anulado frente a otra disposición en contrario. Por razones de orden público, seguridad nacional o bien común puede mitigarse este derecho, como por ejemplo en el caso de realización de investigaciones policiales que justifican el tratamiento de datos encubierto, atendida la finalidad prevista.

2.5. El derecho a ser informado en los primeros cuerpos normativos rectores.

Las técnicas de recopilación de datos y su acceso asociado representan un riesgo latente desde la perspectiva de los derechos fundamentales de las personas, aspecto que fue advertido hace más de veinticinco años por el Consejo de Europa, que hizo suyo el estudio del objeto y análisis de la protección de datos y la falta de homogeneización de las normas nacionales sobre la materia⁴⁵.

Así surge el primer texto europeo dispuesto a regular la materia y que se denomina Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal suscrito con fecha 28 de enero de 1981, abierto desde esta misma fecha para la ratificación de los Estados miembros y para la

⁴⁵ Antes de la elaboración del Convenio confeccionado por el Consejo, la protección de los datos de carácter personal ya habría sido objeto de regulación en diversos países a través de una norma de carácter general o disposiciones sectoriales.

adhesión de países no europeos, sentando los principios fundamentales a observar como los principios de calidad, seguridad, transparencia, entre otros.

El Convenio no constituyó un cuerpo normativo de desarrollo aislado, sino que por el contrario, materializó los trabajos relativos a la materia que se vinieron desarrollando por la Comisión Consultiva desde 1967 y que se plasmaron en las Resolución 509 de “los derechos humanos y los nuevos logros científicos y técnicos” y las resoluciones (73) 22 y (74) 29 que aportan una serie de principios y derechos que siguen influyendo en las legislaciones de hoy en día.

Más tarde, el 24 de octubre de 1995 el Consejo aprobó la Directiva 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos. La Directiva estableció un modelo de acción común para los sistemas de tratamiento de datos, promoviendo los derechos fundamentales consagrados en las constituciones y en las leyes, y favoreciendo la libre circulación de los datos entre los Estados que garanticen un adecuado nivel de protección, más intenso que aquel consagrado por el Convenio.

El Convenio 108 y la Directiva 95/46 establecieron los principios generales y la base de referencia que, incluso, hoy en día se plantean los distintos poderes legislativos nacionales en la tarea de promulgar disposiciones legales capaces de reglamentar los aspectos más relevantes en el tratamiento de datos personales. A través de la observancia, en mayor o menor grado, a este marco procuran ponderar de la mejor forma posible la tensión existente entre la actividad informativa y la defensa de los derechos vulnerables en el mercado de la información.

2.5.1. Convenio 108.

Otorgar facultades de control al titular de los datos, materializadas en un derecho a ser informado, no es una premisa reciente. Como señalábamos, ya hace varias décadas que este punto ha sido objeto de análisis por el Consejo de Europa que estableció los

primeros cuerpos normativos rectores que pretendieron guiar la tarea legislativa que debían emprender las naciones del mundo.

El Convenio 108 que se estableció en miras de la necesidad de ampliar la protección de los derechos y libertades del ser humano y conciliarlas con la libre circulación de información entre los Estados miembros, incluyéndose, simultáneamente, a los Estados no miembros que quisieran ratificar el acuerdo.

El Convenio, tuvo una fuerte influencia en la dictación de leyes de protección de datos adoptadas con posterioridad en los países europeos que a la fecha carecían de normativa. Por otra parte, su flexibilidad y adaptación a las nuevas tecnologías han hecho que muchos de los principios que consagró sigan conservando su valor para la protección de datos personales⁴⁶.

Este cuerpo normativo dispone en su artículo 8 bajo el título de garantías complementarias para la persona concernida, el derecho a ser informado en sus diferentes manifestaciones, así proclama:

i. El derecho a ser informado manifestado en el derecho a conocer la siguiente información:

- La existencia de un fichero automatizado donde consten sus datos personales.
- Las finalidades principales que trascienden el tratamiento de los datos personales.
- La identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero.

ii. El derecho a ser informado manifestado en el derecho a obtener a intervalos razonables y sin demora o gastos excesivos la siguiente información:

⁴⁶ ANGUIITA Ramírez, Pedro, La Protección de Datos Personales y el Derecho a la Vida Privada, Régimen Jurídico, Jurisprudencia y Derecho Comparado, Santiago, Editorial Jurídica de Chile, 2007, Pág. 498.

- La confirmación de la existencia o inexistencia del fichero de datos personales que conciernan a la persona.
- La comunicación de dichos datos en forma inteligible.

iii. El derecho a ser informado manifestado en el derecho a obtener cuando corresponda:

- La rectificación de los datos personales.
- El borrado de los datos personales.

Se dispone que el derecho a obtener la rectificación y el borrado de datos personales, procederá cuando éstos se hayan tratado con infracción a las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del Convenio, de calidad de los datos y de tratamiento de datos sensibles, correspondientemente.

iv. El derecho a ser informado manifestado en la disposición de un recurso si no se ha atendido a la petición de confirmación, de comunicación, de ratificación o de borrado.

El Convenio señala que estos derechos no admitirán excepciones, salvo que éstas constituyan una medida necesaria en una sociedad democrática, es decir, para la protección de la seguridad del Estado, de la seguridad pública, los intereses monetarios del Estado o para la represión de infracciones penales; y, para la protección de la persona concernida y de los derechos y libertades de otras personas.

Asimismo, podrán preverse restricciones para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Además, cada Estado se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los

principios básicos para la protección de datos, entre los que se encuentra el derecho del titular de los datos a ser informado.

2.5.2. Directiva 95/46.

Diez años más tarde de que entrará en vigencia el Convenio 108 del Consejo de Europa, la Unión Europea confecciona un nuevo texto de referencia para orientar el actuar de los Estados, estableciendo un marco regulador más exigente que equilibre el nivel elevado de protección de la vida privada de las personas y la libre circulación de los datos, poniendo énfasis en que para la eliminación de los obstáculos a ésta libre circulación, el nivel de los derechos y libertades de las personas debe ser equivalente en todos los Estados miembros. Así nace la Directiva 95/46/CE que fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los datos.

Una de las fortalezas más importantes de la Directiva para instar a la ratificación de los Estados miembros y los Estados no miembros, consiste en que se rechaza la transferencia de datos personales a países terceros que no garanticen un nivel de protección adecuado de conformidad a las normas establecidas por el texto de la Directiva.

En base a 92 considerandos, la Directiva adopta el nivel de protección que se considerara adecuado, estableciéndose en su capítulo II las condiciones generales para la licitud del tratamiento de datos personales, en cuya sección IV, V y VI se consagran los derechos de información del interesado en sus distintas manifestaciones:

- i. El derecho a ser informado en caso de obtención de datos recabados del propio interesado.

Los Estados miembros deben disponer que el responsable del tratamiento o su representante comuniquen a la persona de quien se recaben los datos que le conciernan, por lo menos la siguiente información, salvo si la persona ya hubiera sido informada de ello:

- a. La identidad del responsable del tratamiento y, en su caso, de su representante.
 - b. Los fines del tratamiento de que van a ser objeto los datos.
 - c. Cualquier otra información tal como:
 - Los destinatarios o las categorías de destinatarios de los datos.
 - El carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder.
 - La existencia de derechos de acceso y rectificación de los datos que le conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
- ii. El derecho a ser informado en caso de obtención de datos que no han sido recabados de propio interesado.

Cuando los datos no hayan sido recabados del interesado, los Estados miembros deberán disponer que el responsable del tratamiento o su representante informen, desde el momento del registro de los datos o, a más tardar, en el momento de la primera comunicación de datos, en el caso de que se piense comunicar datos a un tercero, por lo menos la siguiente información, salvo si el interesado ya hubiera sido informado de ello:

- a. La identidad del responsable del tratamiento y, en su caso, de su representante.
- b. Los fines del tratamiento de que van a ser objeto los datos.

c. Cualquier otra información tal como:

- Las categorías de los datos de que se trate.
- Los destinatarios o las categorías de destinatarios de los datos.
- La existencia de derechos de acceso y rectificación de los datos que le conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Los derechos de información de i) y ii) no se aplicarán cuando:

- Estemos ante un tratamiento con fines estadísticos o de investigación histórica o científica.
- La información al interesado resulte imposible o exija esfuerzos desproporcionados.
- El registro o la comunicación a un tercero estén expresamente prescritos por ley.

En estos tres casos, los Estados miembros establecerán las garantías apropiadas.

iii. El derecho a ser informado manifestado como derecho de acceso.

Los Estados miembros deberán garantizar a todos los interesados el derecho a que se les comunique por el responsable del fichero de forma libre, sin restricciones, ni retrasos o gastos excesivos la siguiente información:

a. La confirmación de la existencia o inexistencia del tratamiento de datos personales que le conciernen, así como por lo menos los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos.

b. Los datos objeto de tratamiento, así como toda la información disponible sobre el origen de los datos.

c. La lógica utilizada en los tratamientos automatizados de sus datos, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15 y que dicen relación con el derecho que los Estados miembros reconocen a las personas a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

iv. El derecho de información manifestado como derecho de consulta ante la autoridad de control.

De acuerdo al principio de publicidad de los tratamientos que se consagra en el artículo 21 de la Directiva, los Estados miembros deben adoptar las medidas necesarias para garantizar la publicidad de los tratamientos, estableciéndose dos modalidades de publicidad:

1) Los Estados miembros deben instar a que la autoridad de control lleve un registro de los tratamientos notificados por los responsables de los registros de datos o, en su caso, su representante. A través de estas notificaciones los distintos responsables de los ficheros comunican a la autoridad de control que realizarán un tratamiento de datos. La notificación debe realizarse con anterioridad a la realización del tratamiento o del conjunto de tratamientos, total o parcialmente, destinados a la consecución de un fin o de varios fines conexos.

Este registro podrá ser consultado por cualquier persona, debiendo informarse a lo menos los siguientes puntos:

- a. El nombre y la dirección del responsable del tratamiento y, en su caso, de su representante.
 - b. El o los objetivos del tratamiento.
 - c. Una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento.
 - d. Los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos.
 - e. Las transferencias de datos previstas a países terceros.
- 2) Cuando los Estados miembros puedan disponer de la simplificación u omisión de la notificación, de acuerdo a lo previsto en el artículo 18.2, los responsables del tratamiento u otro órgano designado por los Estados miembros, deberán comunicar, en la forma adecuada, a toda persona que lo solicite, a lo menos las siguientes informaciones al menos las letras a, b, c, d y e del número anterior.

Para el cumplimiento de los derechos de información en sus distintas modalidades la Directiva establece diferentes medios procesales para que los titulares de los datos hagan valer los derechos otorgados. Estos medios estarán a cargo de la autoridad de control y de la autoridad judicial.

Se establece que la autoridad procesal debe disponer de la capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva y en caso que proceda el conocimiento de la autoridad judicial por aquellos incumplimientos.

Así, la autoridad de control debe recibir las solicitudes de cualquier persona, o cualquier asociación que la represente, en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Y sin perjuicio, de la

presentación de un eventual recurso administrativo, debe concederse al afectado la facultad de interponer recursos judiciales en caso de violación de los derechos que le garanticen las disposiciones del derecho nacional.

v. El derecho de información manifestado como derecho de rectificación, supresión o bloqueo.

Los Estados miembros deberán garantizar a todos los interesados, el derecho a obtener del responsable del tratamiento la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos.

Asimismo, los Estados miembros deberán notificar estas modificaciones a aquellos terceros a quienes se hayan comunicado los datos que están siendo objeto de rectificación, supresión o bloqueo, siempre que no resulte imposible o suponga un esfuerzo desproporcionado.

El ejercicio de estos derechos de información en sus distintas manifestaciones puede ser objeto de medidas legales que establezcan su excepción o limitación, por razones de:

- a. Seguridad del Estado.
- b. Defensa pública.
- c. Seguridad pública.
- d. Prevención, investigación, detección y represión de infracciones penales o de infracciones de la deontología en las profesiones reglamentadas.
- e. Un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales.

f. Una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e).

g. Protección del interesado o de los derechos y libertades de otras personas.

Los Estados miembros podrán limitar, mediante una disposición legal, los derechos de información manifestados como derechos de acceso y derechos a solicitar rectificación, supresión y bloqueo, en los casos en que ostensiblemente no exista ningún riesgo de atentado contra la intimidad del interesado, y los datos:

- Se vayan a tratar exclusivamente con fines de investigación científica.
- Se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

CAPÍTULO III.

CONFIGURACIÓN DEL CONTROL DE DATOS PERSONALES Y DEL DERECHO A SER INFORMADO EN LA LEGISLACIÓN COMPARADA Y CHILE.

3.1. LEGISLACIÓN COMPARADA.

A fin de brindar un panorama sobre la forma en que ingresó y se fue enraizando el derecho a controlar los datos personales y el derecho a ser informado en las diferentes legislaciones de los países del mundo, analizaremos la situación de éstos desde diferentes perspectivas, si han incorporado constitucionalmente disposiciones específicas, si han optado por la incorporación de disposiciones sub constitucionales, o bien, si han preferido ambas opciones simultáneamente.

Internacionalmente se han identificado al menos cuatro modelos de sistemas de regulación para proteger los datos personales: disposiciones constitucionales, leyes generales, leyes sectoriales y autorregulación. En muchos países se recurre a una mixtura complementaria de estos modelos para garantizar un nivel mínimo de protección a los ciudadanos frente al tratamiento de datos personales⁴⁷.

Países como Estados Unidos, han optado por establecer varias normas sectoriales, en lugar de disposiciones generales. Así, por ejemplo se han dictado, entre otras, las siguientes normas: *The Fair Credit Reporting Act* de 1970; *The Electronic Communications Privacy Act* de 1986; *The Health Insurance Portability and Accountability Act* de 1996; *The Gramm – Leach – Bliley Act* de 1999. Sólo a raíz de la previsión europea que impide la transferencia de datos hacia países que no garanticen niveles adecuados de protección a los mismos, Estados Unidos se vio forzado a dictar en el año 2000 los *International Safe Harbor Privacy Principles*, a fin de lograr ser

⁴⁷ DEFENSORÍA DEL PUEBLO COLOMBIANO, Memorias del foro sobre Protección de datos Personales y Regulación Legal del Hábeas Data, Dirección Nacional de Promoción y Divulgación de Derechos Humanos, Bogotá, 2004, Pág. 54.

catalogado por la Unión Europea como un país que garantiza un nivel adecuado de protección de datos.

Aún así, las directrices consagradas por los *International Safe Harbor Privacy Principles* son amplísimas, estableciendo siete principios fundamentales: *notice*⁴⁸, *choice*⁴⁹, *onward transfer*⁵⁰, *security*⁵¹, *data integrity*⁵², *access*⁵³ y *enforcement*⁵⁴. Estos

⁴⁸ Este principio consagra el derecho a ser informado que detenta el titular de los datos. Así señala que una organización que realice tratamiento de datos personales debe informar a los individuos sobre los objetivos para los cuales se está recogiendo información sobre ellos, sobre el mecanismo para ponerse en contacto con la organización por cualquier pregunta o quejas, sobre los terceros a los cuales se les revelará la información, y las opciones que se ofrecen a los individuos para limitar el empleo y utilización de sus datos. Deberá proporcionarse este aviso en lengua clara y visible cuando se les solicite a los individuos proporcionar información personal, o bien, poco tiempo después que la solicitud fue realizada, pero en cualquier caso antes de que la organización use tal información para un objetivo distinto para el cual fue recogida en un comienzo o antes de que ésta sea revelada a un tercero.

⁴⁹ Este principio consagra una facultad similar a lo que vendría siendo para nosotros el derecho a consentir en el tratamiento de datos personales. Establece que la organización que realice tratamiento de datos personales debe ofrecer a los individuos la oportunidad de optar si la información personal que ellos provean pueda ser usada o revelada a terceros (cuando tal uso sea incompatible con el objetivo para el cual fue recogida en un comienzo, o bien, con cualquier otro objetivo revelado al individuo en un aviso). Este derecho a optar debe proporcionarse clara y visiblemente, a través de mecanismos fácilmente disponibles, y económicos para ejercer esta opción. Para la información sensible, es decir, información médica y de salud, la información que revela el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, sobre sindicalizaciones o información que concierne la vida sexual del individuo, el derecho de optar debe ser afirmativo y explícito.

⁵⁰ Este principio establece las normas a seguir en caso de transferencia de datos. Así señala, que una organización sólo puede revelar información personal a terceros cuando esto es compatible con los principios de información (70) y opción (71). Cuando una organización no ha otorgado al titular de los datos el derecho a optar porque el uso es compatible con el objetivo para el cual los datos fueron recogidos en un comienzo, o bien, porque la transferencia fue informada, si la organización desea transferir los datos a un tercero, esto podrá realizarse siempre y cuando el tercero esté suscrito a los principios de “puerto seguro” o firme un acuerdo escrito a través del cual se comprometa a proporcionar al menos un nivel de protección adecuado en atención a los principios de “puerto seguro”.

⁵¹ Este es el principio de seguridad en el tratamiento de datos personales que señala que tanto en la creación de organizaciones, su mantenimiento, el uso y la diseminación de la información personal se deben tomar las medidas razonables para asegurar la fiabilidad de su empleo intencionado, tomando las precauciones razonables para proteger la pérdida, el mal uso y el acceso no autorizado, la revelación, la alteración y la destrucción.

⁵² Este es el principio de integridad de los datos, según el cual una organización sólo puede tratar la información personal de conformidad a los objetivos para los cuales ha sido recogida. Para el cumplimiento de estos objetivos, la organización deberá tomar las medidas razonables para asegurar que los datos son exactos, completos y actuales.

⁵³ Este principio corresponde al derecho de acceso que detenta el titular de los datos, según el cual los individuos deben tener el acceso [razonable] a la información personal que una organización posee sobre ellos, siendo capaces de corregir o enmendar aquella información cuando sea inexacta. [El acceso razonable depende de la naturaleza y la

principios sintetizan las garantías dispuestas por la Directiva 95/46, incluyendo el derecho a ser informado, el derecho a consentir en el tratamiento, el derecho a acceder a los datos y solicitar corrección o enmienda de la información inexacta.

Estados Unidos ha optado por este régimen porque promueve la autorregulación con miras a que los responsables de los bancos de datos establezcan sus propios códigos de conducta o “códigos de honor” que se comprometen a cumplir frente a sus clientes respecto a sus datos personales. Sin embargo, internacionalmente este mecanismo ha sido cuestionado por la falta de efectividad y cumplimiento por parte de las compañías⁵⁵.

Otros países optaron por consagrar en sus Cartas Fundamentales el derecho de protección de los datos personales y específicamente el derecho del titular de los datos a controlar la información que le concierne. Constituciones como la de Portugal, Alemania y España, establecieron estas facultades, con diferentes matices. Mientras, en América Latina, el primer país en incorporar constitucionalmente disposiciones específicas fue Guatemala que en su Constitución de 1985, dispuso:

“Artículo 31: Toda persona tiene derecho de conocer lo que de ella conste en archivos o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan

sensibilidad de la información, su empleo, y el costo y la dificultad de proporcionar al individuo el acceso a la información.]

⁵⁴ Este principio de aplicación o ejecución señala que la protección eficaz de la intimidad debe incluir mecanismos para asegurar el cumplimiento de los principios de “puerto seguro”, contemplándose recursos para los individuos que se vean afectados por el incumplimiento de estos los principios, y consecuencias para la organización cuando no observe estos principios. Se señala que como mínimo, tales mecanismos deben incluir: a) recursos con mecanismos fácilmente disponibles, económicos e independientes por los cuales las quejas de un individuo y discusiones pueden ser investigadas y resueltas. Asimismo, los daños y perjuicios puedan ser concedidos cuando las iniciativas sectoriales aplicables de la ley o privadas los provean; (b) procedimientos para verificar que las atestiguaciones y aseveraciones sobre prácticas de intimidad son verdaderas y que las prácticas de intimidad han sido reveladas; (c) obligaciones de remediar problemas que provienen del fracaso del cumplimiento de estos principios por organizaciones que anuncian su adhesión a ellos y consecuencias para tales organizaciones. Las sanciones deben ser suficientemente rigurosas para asegurar el cumplimiento de los principios consagrados.

⁵⁵ ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), Privacy & Human Rights: An international survey of privacy laws and development, Washington, EEUU, 2002, Pág. 4.

prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos”.

Como señalábamos, algunos países, simultáneamente al establecimiento del derecho a controlar los datos personales a nivel constitucional, dotaron a sus sistemas legales de disposiciones generales que desarrollaran estos derechos y permitieran su adecuado ejercicio.

Pasaremos a analizar, entonces, los casos de algunos países y la forma en que éstos han establecido el derecho a controlar los datos personales y a ser informado en sus Constituciones y en sus leyes generales. Estudiaremos en primer lugar, el caso de España, atendido el alto grado de influencia que traspasó a Latinoamérica, para luego proceder al análisis de las legislaciones de Argentina, Colombia y México.

3.1.1. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución española y en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

La Norma Fundamental española se convirtió, con la inclusión del artículo 18.4, en el segundo texto constitucional, tras la Constitución portuguesa de 1976, que reconoce a través del máximo rango legal, la necesidad de tutelar los derechos de las personas frente a las nuevas técnicas de la informática. Así, el texto del artículo 18.4 señala:

“18. 4. 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”.

Pese a que el enfoque consagrado pareciera plasmar sólo el aspecto limitativo y restrictivo del fenómeno, el precepto no pretende impedir el uso de la informática, sino

que busca hacerla compatible con el respeto de los derechos fundamentales, eliminando los riesgos de un manejo abusivo de los datos personales.

El artículo 18.4 de la Constitución se ha puesto en conexión con el artículo 10.5 b) de la Constitución española, el cual señala:

“La ley regulará:

b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad nacional y defensa del Estado, la averiguación de los delitos y la intimidad de las personas”.

Se ha querido ver en este precepto constitucional, el complemento del que carece el artículo 18.4 en relación con una visión positiva y social del fenómeno⁵⁶, sin embargo, esta interpretación no sería acertada por varios motivos, entre los que se encuentran, que sólo se refiere al acceso a registros administrativos, sin extenderse a los ficheros de titularidad privada; y, que realmente no tiene como misión preservar ningún derecho fundamental de los ciudadanos, sino simplemente, garantizar el derecho de acceso y la transparencia en la actuación de la administración.

La única coincidencia que comparten en cuanto a su texto es la alusión a la intimidad como límite, sin embargo, dada su ubicación en la Carta Fundamental se deduce que sólo el artículo 18.4 se posiciona dentro del catálogo de derechos fundamentales y libertades públicas, específicamente en el extenso terreno de la intimidad.

Pese a que no es un punto pacífico ni en doctrina ni en jurisprudencia, no existiría una dependencia material entre el derecho a la intimidad y el derecho consagrado en el

⁵⁶ SERRANO Pérez, María Mercedes, El derecho fundamental a la protección de datos. Derecho español y comparado, Thompson, Civitas, Madrid, España, 2003, Pág. 127.

artículo 18.4⁵⁷, ya que su inciso final promueve como límite de la informática, el ejercicio del entramado de derechos fundamentales que consagra la Constitución. Este ejercicio se verá satisfecho a través de las facultades que integran el elemento positivo que detenta el titular de los datos y que, como ya vimos, se dictaminó por el Tribunal Constitucional a través de la sentencia 254/1993⁵⁸ la que habla incluso de un nuevo derecho fundamental a controlar y disponer de la información personal automatizada⁵⁹.

De las palabras del Tribunal se deduce una parte esencial del contenido del derecho, esto es, la necesidad de conocer, acordar y consentir las operaciones a que pueden ser sometidos los datos personales de los individuos. Lo importante aquí es recalcar que el artículo 18.4 complementado con los instrumentos interpretativos fundamentales como lo son el Convenio 108 del Consejo de Europa y la Directiva 46/95, fijan el contenido esencial del derecho a la protección de datos personales que se configura por un conjunto de derechos de control que garantizan la protección de la persona frente al manejo de la información que le concierne

El control, por parte del individuo, se desarrollaría en dos momentos, en relación con los datos personales. En un primer momento se trataría de un control-autodecisión, que se agota en el propio acto por medio del cual el individuo decidiría la entrega o no de sus datos, es decir, ejercería un dominio sobre la revelación de sus informaciones

⁵⁷ El Anteproyecto Constitucional establecía, efectivamente, una dependencia material pues mencionaba exclusivamente la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos.

⁵⁸ Fragmento sentencia 254/1996: "...Nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental..."

⁵⁹ Esta afirmación se confirma por la sentencia del Tribunal Constitucional 292/2000 que señala: "Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular".

personales. En un segundo momento, el individuo controlaría el tratamiento a que los mismos son sometidos, sería una autodisposición sobre su uso concreto⁶⁰.

En este sentido, el artículo 18.4 de la Constitución española, desarrollado en la Ley Orgánica 15/1999 de fecha 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) que derogó la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y que establece la libertad informática traducida en un derecho de control, se sustenta en dos pilares fundamentales: el consentimiento y los derechos que hacen practicables este consentimiento y que determinan las facultades que posibilitan el ejercicio del derecho fundamental y garantizan su protección.

Para la efectiva tutela de los derechos legalmente consagrados se creó la Agencia Española de Protección de Datos, nacida en 1994 como órgano de control creado en cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal. Su sede está en Madrid y tiene un ámbito de actuación que abarca toda España.

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de la administración pública en el ejercicio de sus funciones. Vela por el cumplimiento de la legislación de protección de datos por parte de los responsables de los ficheros.

Simultáneamente, existen otras agencias de protección de datos de carácter autonómico en la Comunidad de Madrid, Cataluña y en el País Vasco; con un ámbito de actuación limitado a los ficheros públicos que existan en sus respectivas Comunidades Autónomas. Entre estas, destaca la Agencia de Protección de Datos de la Comunidad de Madrid, que es una autoridad independiente de control que garantiza y protege el derecho fundamental a la protección de datos personales. Sus

⁶⁰ SERRANO Pérez, María Mercedes, El derecho fundamental a la protección de datos. Derecho español y comparado, Madrid, Thompson, Civitas, 2003, Pág. 184.

competencias versan sobre los ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, Entes que integran la Administración Local de su ámbito territorial, Universidades públicas y Corporaciones de derecho público representativas de intereses económicos y profesionales de la misma, en este último caso, siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.

Tanto la Agencia Española de Protección de Datos como las Agencias de las distintas Comunidades Autónomas, tienen como misión fundamental la cautela de los derechos consagrados en la LOPD. Nos referiremos, en particular, al derecho a ser informado en sus distintas manifestaciones a lo largo de la legislación española.

1. Derecho a ser informado en toda solicitud de datos personales.

El artículo 5 N^o 1 de la LOPD se refiere al derecho de información que asiste al titular de los datos personales cuando la información a tratar se recabe de su propia persona. En estos casos el titular debe ser informado de forma expresa, precisa e inequívoca sobre los siguientes aspectos:

- a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Además, será obligatorio designar un representante en España para que dé cumplimiento al deber de información cuando:

- El responsable del tratamiento no se encuentre establecido en el territorio comprendido por la Unión Europea.
- Utilice en el tratamiento de datos personales medios situados en territorio español. Con excepción si tales medios se utilizan con fines de tránsito.

Cabe hacer dos advertencias:

- i. Si en la recogida de datos personales se utilizan cuestionarios u otros impresos, en estos mismos deberá figurar legiblemente la información de las letras a), b), c), d) y e).
- ii. Si de la naturaleza de los datos que se solicitan o de las circunstancias en que éstos se recaban, puede deducirse el contenido de los aspectos a informar de las letras b), c) y d), no será necesaria su información al titular precisa, expresa e inequívocamente.

2. Derecho a ser informado cuando los datos personales se recaben de terceros.

De acuerdo al artículo 5 N° 4 de la LOPD, cuando los datos personales no hayan sido recogidos de su titular sino de terceras personas u órganos, deberá informarse al titular expresa, clara e inequívocamente, por el responsable del fichero o su representante de los siguientes puntos:

- a. Del contenido del tratamiento.
- b. De la procedencia de los datos.

- c. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

El responsable del fichero o su representante deberán dar cumplimiento a estas disposiciones dentro del plazo de tres meses siguientes al momento del registro, salvo que ya hubiera sido informado con anterioridad.

3. Derecho a ser informado manifestado como derecho de consulta al Registro General de Protección de Datos.

Una de las funciones de la Agencia de Protección de Datos española consiste en velar por la publicidad de la existencia de los ficheros de datos de carácter personal. Para cumplir este principio la Agencia contiene un órgano integrado denominado Registro General de Datos, que consiste en una nómina que se constituye a través de las notificaciones que realizan las personas o entidades que proceden a la creación de ficheros de datos de carácter personal.

De acuerdo al derecho contemplado en el artículo 14 de la LOPD, cualquier persona podrá conocer, recabando la información oportuna del Registro General de Protección de Datos, de consulta pública y gratuita:

- a. La existencia de tratamiento de datos de carácter personal.
- b. Las finalidades del tratamiento de datos de carácter personal.

c. La identidad del responsable del tratamiento.

4. Derecho a ser informado manifestado como derecho de acceso⁶¹.

Como señala el autor español Pablo Lucas Murillo de La Cueva el derecho de acceso es el derecho que concede al interesado:

“La posibilidad de comprobar si se dispone de información sobre uno mismo y conocer el origen del que procede la existente y la finalidad con que se conserva. Del mismo modo, el derecho de acceso conlleva la facultad de exigir y obtener una comunicación escrita en la que consten los anteriores extremos⁶²”.

De acuerdo al artículo 15 de la LOPD, el titular de los datos tendrá derecho a solicitar y obtener gratuitamente, a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo al efecto, la siguiente información:

a. De sus datos de carácter personal sometidos a tratamiento.

b. Del origen de sus datos sometidos a tratamiento.

c. De las comunicaciones realizadas o que se prevén hacer de los datos sometidos a tratamiento.

La información de a), b) y c) podrá obtenerse por la mera consulta de los datos por medio de visualización, o la indicación de los datos que son objeto de tratamiento

⁶¹ Como señala FREIXAS Gutiérrez, G., La protección de los datos de carácter personal en el derecho español, Barcelona, Bosh, 2001, Pág. 191. Este autor distingue entre el derecho de acceso del artículo 15 y el derecho de publicidad general, anteriormente descrito, del artículo 14.

⁶² LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la autodeterminación informativa, Temas Claves de la Constitución Española, Madrid, Edición Tecnos, Pág. 187.

mediante escrito, copia, telecopia o fotocopia, certificada o no, de forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos, constituyendo una lista cerrada⁶³. La elección de cualquiera de ellas dependerá de la necesidad del titular de la información, aunque habrá que atender también a las posibilidades físicas del propio tratamiento. Si no existe un impedimento de estas características será el afectado quien decidirá si estima conveniente realizar una visualización del fichero u obtener copia del mismo sin que el responsable pueda oponerse a ninguna modalidad de información⁶⁴.

La forma de ejercitar el derecho de acceso, según el artículo 17 de la LOPD, será establecida reglamentariamente. Los artículos 24 y 25 del Real Decreto 1720/2007, desarrollan el procedimiento aplicable para el ejercicio de los derechos de acceso, rectificación, eliminación y bloqueo, especificándose el ejercicio del derecho de acceso en el artículo 28⁶⁵. El acceso se iniciará, a tenor del artículo, con una petición o

⁶³ HERRÁN Ortiz, Ana Isabel, La violación de la intimidad en la protección de datos personales, Madrid, Dykinson, Pág. 283.

⁶⁴ FREIXAS Gutiérrez, G., La protección de los datos de carácter personal en el derecho español, Barcelona, Bosh, 2001, Pág. 192.

⁶⁵ Artículo 28. Ejercicio del derecho de acceso.

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- a) Visualización en pantalla.
- b) Escrito, copia o fotocopia remitida por correo, certificado o no.
- c) Telecopia.
- d) Correo electrónico u otros sistemas de comunicaciones electrónicas.

Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.

3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

solicitud dirigida al responsable del fichero, con fórmula oficial, identificando claramente al interesado y el fichero a consultar. El precepto vuelve a repetir las distintas modalidades de consulta que ya recoge la ley y cuya elección se condiciona, como señalábamos, a las singularidades del fichero y a las necesidades del afectado⁶⁶.

La fórmula para ejercitar el derecho de acceso consta en un modelo editado por la Agencia Española de Protección de Datos⁶⁷.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

⁶⁶ SERRANO Pérez, María Mercedes, El derecho fundamental a la protección de datos. Derecho español y comparado, Madrid, Thompson, Civitas, 2003, Pág. 354.

⁶⁷ A. DERECHO DE ACCESO.

A.1. EJERCICIO DEL DERECHO DE ACCESO (1).

DATOS DEL RESPONSABLE DEL FICHERO (2).

Nombre / razón social: Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza nº C.Postal
Localidad Provincia Comunidad Autónoma
C.I.F./D.N.I.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL(3).

D./ D^a., mayor de edad, con domicilio en la C/Plaza nº....., Localidad
Provincia C.P. Comunidad Autónoma con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

5. Derecho a ser informado manifestado como derecho de rectificación y cancelación.

La consecuencia de acceder a los datos y conocer su estado y sus circunstancias condiciona al paso siguiente. Una vez que el afectado ha tomado conocimiento sobre sus datos personales, que constan en determinado registro, puede suceder que el estado de los datos sea correcto y su tratamiento se ajuste a la ley. En cuyo caso el titular de los datos ha hecho efectivo su derecho a la libertad informática, conociendo y controlando sus informaciones personales, y el uso que de las mismas se hace. Sin embargo, puede suceder lo contrario, es decir, que el conocimiento de los datos revele alguna inexactitud, carencia o incumplimiento de las obligaciones derivadas de la Ley Orgánica 15/1999.

Así, para que el derecho de acceso sea eficaz, cuando los datos son inexactos, incompletos o su tratamiento no se ajusta a la ley, el afectado tendrá derecho a solicitar su rectificación o cancelación de acuerdo a lo señalado por el artículo 16.2 de la LOPD. La inexactitud o carencia se soluciona mediante la rectificación, mientras que la falta de cumplimiento de la ley ocasionaría la cancelación o borrado.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

Ena.....de.....de 20.....

Firmado

(1) Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.

(2) Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

(3) También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

Es muy importante recalcar que la Agencia, a través de la Instrucción 1/98, ha afirmado con rotundidad que pese a la relación que existiría entre los derechos de acceso y los derechos de rectificación y cancelación, estos tres derechos son independientes, atendiendo tanto a sus objetivos como a sus resultados, no existiendo conexión entre ellos:

“Norma primera. 2. La ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro”.

Al igual que lo que ocurre con el derecho de acceso, el de rectificación y cancelación se convierten en una carga que recae en el responsable del fichero. Así, una vez realizada la solicitud de rectificación o cancelación, el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho del afectado en el plazo de diez días⁶⁸.

La cancelación producirá el bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Una vez cumplido este plazo deberá procederse a la supresión.

Cuando los datos rectificadas o cancelados hayan sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

⁶⁸ El plazo contemplado en la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (Vigente hasta el 14 de enero de 2000) era de cinco días. La modificación legislativa responde, sin duda, a la experiencia que demostró que plazo de cinco días no era un plazo razonable en atención al trabajo del responsable y a la complejidad del proceso de rectificación y cancelación.

Para ejercer los derechos de rectificación y cancelación, no se exigirá contraprestación alguna a cambio.

6. Derecho a ser informado en la prestación de servicios de información sobre solvencia patrimonial.

El artículo 29 de la LOPD sobre protección de datos señala que cuando se traten datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitadas por el acreedor o por quién actúe por su cuenta o interés, deberá notificarse a los titulares de los datos registrados, en el plazo de treinta días desde dicho registro, una referencia de los datos que hubieren sido incluidos, informándosele además de su derecho a recabar información sobre la totalidad de los datos del registro, en los términos que establece la ley.

Así, cuando el afectado lo solicite, el responsable del tratamiento les comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado sus datos.

7. Derecho a ser informado en los tratamientos de datos con fines de publicidad y de prospección comercial.

De acuerdo al artículo 30 de la LOPD quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizando nombres y direcciones u otros datos de carácter personal, cuando figuren en fuentes accesibles al público, de conformidad a lo establecido en el párrafo segundo del artículo 5.5 de la ley, deberán informar al titular de los datos, en cada comunicación, sobre el origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Cuando el titular de los datos ejerza el derecho de acceso, gozará de la facultad de conocer el origen de sus datos de carácter personal, así como del resto de la información que señala el artículo 15 de la LOPD.

El titular tendrá derecho a oponerse al tratamiento de los datos que le conciernan, previa petición y sin gastos, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Limitaciones al derecho a ser informado en sus distintas manifestaciones.

De acuerdo al artículo 5.5 y 22 de la LOPD, no se aplicarán los derechos de información en sus distintas modalidades, cuando:

- a. Expresamente una ley lo prevea.
- b. Cuando el tratamiento tenga fines históricos, estadísticos o científicos.
- c. Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración a:
 - El número de interesados.
 - La antigüedad de los datos.
 - las posibles medidas compensatorias.
- d. De acuerdo a los casos del artículo 22 N° 2, 3 y 4 (ficheros creados por las Fuerzas y Cuerpos de Seguridad para fines policiales) se pueda denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

e. De acuerdo al artículo 22 N° 4 los responsables de los ficheros de la Hacienda Pública estimen que el ejercicio de los derechos obstaculiza las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias o el afectado esté siendo objeto de actuaciones inspectoras.

f. La información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.

La legislación española estableció como órgano de control a la Agencia Española de Protección de Datos Personales, otorgándole diversas facultades, entre las que se encuentran:

- i. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- ii. Emitir las autorizaciones previstas en la ley o en sus disposiciones reglamentarias.
- iii. Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la ley.
- iv. Atender las peticiones y reclamaciones formuladas por las personas afectadas.
- v. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

vi. Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajusten a sus disposiciones.

vii. Ejercer la potestad sancionadora en los términos previstos por el Título VII de la ley.

viii. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

ix. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales⁶⁹.

Como decíamos, en el ejercicio de estas facultades la Agencia Española de Protección de Datos Personales conoce las actuaciones que contraríen las disposiciones de la LOPD y, especialmente, aquellas que constituyan un incumplimiento de los derechos por parte de los interesados. Así, los titulares de los datos podrán interponer reclamación cuando se les deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

A través de la reclamación, el afectado pone en conocimiento de la Agencia o, en su caso, del organismo competente de cada Comunidad Autónoma, la infracción a la ley, los que deberán asegurarse de la procedencia o improcedencia de la denegación, dictando resolución expresa de tutela de derechos en el plazo máximo de seis meses.

⁶⁹ Estas son sólo algunas de las facultades que detenta la Agencia Española de Protección de Datos Personales. Las facultades señaladas son las que se vinculan, directa o indirectamente, al derecho a ser informado en sus diferentes manifestaciones.

Contra estas resoluciones de la Agencia procederá recurso contencioso-administrativo.

Simultáneamente, los interesados que, como consecuencia del incumplimiento por parte del responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados, debiendo distinguir:

- Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.
- En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Ahora, volviendo a las facultades de la Agencia Española de Protección de Datos Personales, una vez que ésta verifica la infracción a la ley procederá a imponer sanciones, las que se calificarán como leves, graves o muy graves. En cuanto al derecho a ser informado y sus diferentes manifestaciones se establece que se considera:

i. Infracción leve:

- No atender por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD.

ii. Infracción grave:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el “Boletín Oficial del Estado” o Diario Oficial correspondiente.
- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos que éste sea exigible.
- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción grave.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente LOPD ampara.
- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en la ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquel a tales efectos.
- La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.

- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de la LOPD, cuando los datos hayan sido recabados de persona distinta del afectado.

iii. Infracciones muy graves:

- La recogida de datos en forma engañosa y fraudulenta.

- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

- Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 de la LOPD cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.

- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable, sin autorización del Director de la Agencia Española de Protección de Datos.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición⁷⁰.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

La LOPD establece que las infracciones generan la imposición de sanciones monetarias, fluctuando en los siguientes valores:

- Las infracciones leves son sancionadas con multa de 100.000 a 10.000.000 de pesetas, es decir, alrededor de \$424.348 a \$42.458.322 pesos chilenos⁷¹.
- Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas, es decir, alrededor de \$42.458.322 a \$212.289.011 pesos chilenos.
- Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas, es decir, alrededor de \$212.289.011 a \$424.580.702 pesos chilenos.

La cuantía de estas sanciones se graduará atendiendo a:

- La naturaleza de los derechos personales afectados.
- El volumen de los tratamientos efectuados.
- Los beneficios obtenidos.

⁷⁰ Como señala María Mercedes SERRANO Pérez, El derecho fundamental a la protección de datos. Derecho español y comparado, Madrid, Thompson, Civitas, 2003, Pág. 357. "Cabe hacer una leve objeción a la redacción de esta infracción. De ella se deduce que el supuesto de hecho que ocasiona la conducta infractora es su reiteración, no su simple comisión sin más, según el significado de la fórmula empleada: "de forma sistemática". Desde luego la repetición en una conducta de ese tipo es algo grave, pero no lo es menos si ello se realizara una sola vez. La Ley valoraría, para calificar la sanción, el número de veces que se realiza la conducta, no la importancia de la misma, esto es la cantidad pero no la calidad".

⁷¹ Conversión de moneda calculada según promedio correspondiente a marzo de 2010.

- El grado de intencionalidad.
- La reincidencia.
- Los daños y perjuicios causados a las personas interesadas y a terceras personas.
- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Si, en razón de las circunstancias concurrentes, el órgano sancionador apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

En ningún caso podrá asignarse una sanción más grave que la fijada en la ley para la clase de infracción en la que se integre la que se pretenda sancionar.

Jurisprudencia de la Agencia Española de Protección de Datos y de la Agencia de Protección de Datos de la Comunidad de Madrid.

i. Infracciones al artículo 5 de la LOPD: derecho de información en la recogida de datos.

- RESOLUCIÓN: R/01208/2008. Agencia Española de Protección de Datos. El comité de empresa de la entidad Café Iruña S.A recurre a la Agencia Española de Protección de Datos, señalando que en el interior del “Café Iruña” se han instalado varias cámaras de videovigilancia, tanto en el área de atención al público, como en el área de utilización exclusiva de los empleados. Manifiestan que tienen conocimiento de que las imágenes obtenidas tienen un tratamiento posterior, sin que se haya creado ningún fichero ni se informe adecuadamente a los usuarios ni a los trabajadores. El Director de la Agencia Española de Protección de Datos impone a la entidad CAFÉ IRUÑA S.A., por una infracción del artículo 5 de la LOPD, tipificada como leve en el artículo 44.2.d) de dicha norma, una multa de 601,01 euros, de conformidad con lo establecido en el artículo 45.1,4 de la citada Ley Orgánica.

- RESOLUCIÓN: R/02463/2009. Agencia Española de Protección de Datos. En el garaje de la Comunidad de Propietarios, D.A.A.A. instaló un sistema de vigilancia mediante videocámaras que capta y graba las imágenes de las personas que se encuentran en su interior. El titular de la plaza de garaje es D.A.A.A., la instalación y el mantenimiento de las cámaras de vigilancia se realizan por la empresa de seguridad privada, denominada SYCIGAL, S.L., inscrita en el Registro de Empresas de Seguridad existente en el Ministerio del Interior. En la citada plaza de garaje no se facilita información a los afectados, acerca de la existencia del sistema de videocámaras y del tratamiento de datos personales, en los términos recogidos en los artículos 5 de la LOPD y 3 de la citada Instrucción 1/2006, al carecer de distintivos informativos y/o hojas informativas que contengan la información que se especifica en la citada normativa. El Director de la Agencia Española de Protección de Datos impone a D.A.A.A., por una infracción del artículo 5 en sus apartados 1, 2, 3 de la LOPD, en relación con el artículo 3 de la Instrucción 1/2006, tipificada como leve en el artículo 44.2 d) de dicha norma, una multa 1.500 euros de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica.

- RESOLUCIÓN: R/01974/2009. Agencia Española de Protección de Datos. La edición de agosto de 2008 de la revista HIGH SCHOOL MUSICAL publica en su página 7 un sorteo que promueve PANINI ESPAÑA, S.A. Para participar se incluye un cupón que hay que remitir con los datos personales. Este cupón no incluye la cláusula informativa prevista en el artículo 5 LOPD. PANINI ESPAÑA, S.A. ha manifestado que el número de la revista objeto de la denuncia, debido a un error no incluía la siguiente leyenda: “Se comunica al padre/madre/tutor que los datos consignados en este cupón quedarán recogidos en un fichero temporal bajo la responsabilidad de Panini España S.A. Los datos serán utilizados únicamente para el envío de los correspondientes premios y eliminados una vez finalice la promoción. Promoción válida hasta el 30 de septiembre”. Manifiesta también que, respecto al número de la revista denunciado, del texto del anuncio se deduce claramente la naturaleza de los datos personales que se solicitan ya que, para participar en un concurso, es necesario conocer la identidad del concursante. Por otra parte, los datos que figuran en el cupón no son objeto de

tratamiento; cuando llega la fecha límite se eligen los dibujos ganadores, se contacta con los padres para enviar el premio y se destruyen todos los cupones, por lo que el período de permanencia de los datos es de unas ocho semanas. Dado que la permanencia de los datos es temporal, el fichero correspondiente no se ha inscrito en el Registro General de Protección de Datos. El Director de la Agencia Española de Protección de Datos impone a la entidad PANINI ESPAÑA, S.A., por una infracción del artículo 5 de la LOPD, tipificada como leve en el artículo 44.2.d) de dicha norma, una multa de 6.000 euros de conformidad con lo establecido en el artículo 45.1 y 4 de la citada Ley Orgánica.

- RESOLUCIÓN: R/01946/2008. Agencia Española de Protección de Datos. Con fecha de 2 de octubre de 2007 tiene entrada en esta Agencia un escrito de doña P.P.P. en el que declara que con fecha 10 de agosto de 2007 realizó una reclamación ante la empresa AUTO-RES, S.L., para lo cual completó un formulario en el que facilitó sus datos de nombre y apellidos, dirección, teléfono y número de D.N.I. La denunciante manifiesta que en el formulario no se facilita ninguna información relativa al tratamiento de los datos personales que se recogen. En el formulario de reclamación aportado por la denunciante no se incluye ninguna leyenda informativa en relación con lo establecido en el art. 5 de la LOPD. AUTO RES S.L. comunicó que la única finalidad de recoger los datos personales de los viajeros que desean formular una reclamación ante la empresa, es la de poder dar contestación a la misma y por ello no han inscrito ficheros de la entidad. El Director de la Agencia Española de Protección de Datos impone a la entidad AUTO RES, S.L., por la infracción del artículo 5 de la LOPD, tipificada como leve en el artículo 44.2.d) de dicha norma, una multa de 601,01 euros de conformidad con lo establecido en el artículo 45.1 de la citada Ley Orgánica.

- Agencia de Protección de Datos de la Comunidad de Madrid. D.XXXX, presentó una denuncia ante la Agencia, en la cual ponía de manifiesto que se había puesto en marcha en todos los hospitales públicos de la Comunidad de Madrid la utilización de un modelo de recetas para la dispensación de fármacos en las farmacias de los mismos que requería la aportación de una serie de datos de carácter personal de los pacientes, lo que a su juicio vulneraba los derechos a la protección de la intimidad, sin que se

garantizara la confidencialidad de los mismos. Los datos solicitados eran: nombre y apellidos del paciente, número de historia clínica, CIP o código de identificación personal que figura en la tarjeta sanitaria, CIAS médico de familia correspondiente, nombre y dos apellidos del prescriptor, número de colegiado, servicio clínico del médico prescriptor, CIAS del médico prescriptor, diagnóstico, código de la Clasificación Internacional de Enfermedades versión 10 de la Organización Mundial de la Salud, Programa de dispensación, entre los que se encuentra HCC Hepatitis Crónica Genitivo Carga Viral, HIV Tratamiento Antirretroviral Recuento CD4 Carga Vira. El Director de la Agencia de Protección de Datos de la Comunidad de Madrid procedió a declarar que el Hospital había cometido una infracción del artículo 44.2.d) de la LOPD, que califica como infracción leve proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD. Asimismo se instó al citado Hospital a informar en los Documentos de Prescripción y Dispensación de Medicamentos a Pacientes Externos en los términos descritos en el artículo 5 de la LOPD, procediendo a comunicar a esta Agencia de Protección de Datos de la Comunidad de Madrid las medidas que se adopten a estos efectos.

ii. Infracción al artículo 6 de la LOPD: consentimiento del afectado.

- RESOLUCIÓN: R/02449/2009. Agencia Española de Protección de Datos. En fechas 07/08/2007 y 14/08/2007, tuvo entrada en la Agencia Española de Protección de Datos los escritos de D.A.A.A., en el que declara que el 12/06/2003 firmó un contrato de prestación de servicios con EXPERT para la gestión de la cartera de clientes de ESTUDIO, de la que además es cliente, decidiendo posteriormente EXPERT la rescisión del mismo comunicándolo a ESTUDIO; no obstante, siguió tratando los datos de los clientes de la cartera de esta última, vulnerando la normativa vigente en materia de protección de datos. ESTUDIO al tener conocimiento del tratamiento de sus clientes requirió a dicha empresa que procediera a la devolución de su base de datos de clientes y cesara en dicho tratamiento hecho que hasta el momento no se ha producido. El Director de la Agencia Española de Protección de Datos impone a la entidad EXPERT EJECUTIVOS, S.A. por una infracción del artículo

6.1 de la LOPD, tipificada como grave en el artículo 43.3.d) de dicha norma, una multa de 60.101,21 euros de conformidad con lo establecido en el artículo 45. 2 y 4 de esa misma Ley Orgánica, en esa cuantía mínima.

- RESOLUCIÓN: R/02333/2009. Agencia Española de Protección de Datos. Mediante carta de agosto de 2007 el denunciante se dirige a FRANCE TELECOM ESPAÑA, S.A., solicitando la no utilización de sus datos personales para envío de todo tipo de publicidad, “Bien sea por envíos de correo, llamadas telefónicas o visitas al domicilio particular”. FRANCE TELECOM ESPAÑA, S.A., le comunica que tras recibir su solicitud de no utilización o cesión de sus datos personales a terceros con fines comerciales o publicitarios y cumpliendo la normativa, han procedido a llevar a cabo dicha solicitud. Con fecha de 8 de julio de 2008, el denunciante interpone denuncia en la Agencia Española de Protección de Datos, manifestando la no atención de su derecho de oposición por parte de la denunciada y el tratamiento de sus datos sin consentimiento, por haberle enviado publicidad, constando al menos dos envíos publicitarios de mayo y junio de 2008, en los que se utilizan los datos personales del denunciante. El Director de la Agencia Española de Protección de Datos impone a la entidad FRANCE TELECOM ESPAÑA S.A., por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 d) de dicha norma, una multa de 60.101,21 euros de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica.

- RESOLUCIÓN: R/02287/2009. Agencia Española de Protección de Datos. La entidad Comisionado para el Mercado de Tabacos, en ejercicio de las competencias que tiene atribuidas, inició expediente sancionador a doña A.A.A., titular de la expendedoría de tabaco y timbre (#####,*). En dichas actuaciones, la entidad comprobó que doña AAA, emitió cinco facturas a nombre de B.B.B., E.E.E., F.F.F. y G.G.G., sin que ninguno de ellos hubiese sido cliente de la misma. Doña A.A.A., durante la tramitación del presente procedimiento sancionador, declaró que las facturas se emitieron erróneamente a nombre de las personas que habían aportado sus currículos para optar a un puesto de trabajo como dependiente de la expendedoría que aquella administra, consecuencia de un error al imprimir dichas facturas. B.B.B., E.E.E, F.F.F. y

G.G.G., han negado haber facilitado su currículum a doña A.A.A., no habiendo prestado su consentimiento para que éste cediera dicho documento a A.A.A. El Director de la Agencia Española de Protección de Datos impone a doña A.A.A., por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 60.101,21 euros, de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.

- RESOLUCIÓN: R/01261/2009. Agencia Española de Protección de Datos. Con fecha de 18 de noviembre de 2008, el inspector actuante realiza una consulta a la página de Internet <http://#####>, a través de la cual se accede a imágenes tomadas por una cámara de video. La cámara transmite imágenes en tiempo real del interior del establecimiento propiedad de COMUTEL S.A. La instalación y resolución de la cámara permite identificar a las personas que se sitúen en la zona de cobertura de la misma. El visionado de las cámaras es de libre acceso para cualquier usuario de Internet, ya que se ha realizado sin que haya existido ningún tipo de control de acceso previo y con la simple selección de la citada dirección de Internet en el navegador. La dirección IP donde se ha encontrado instalada la cámara, en la fecha y hora en que se han detectado las imágenes, corresponde a un servicio de acceso a Internet cuyo titular es la entidad COMUTEL, S.A. En la fecha de realización del acta notarial de, la cámara denunciada había sido retirada no existiendo ningún dispositivo de grabación. El Director de la Agencia Española de Protección de Datos impone a la entidad COMUTEL, S.A., por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 2.500 euros de conformidad con lo establecido en el artículo 45.2.4. y 5 de la citada Ley Orgánica.

iii. Infracciones al artículo 15 de la LOPD: derecho de acceso.

- RESOLUCIÓN: R/00518/2008. Agencia Española de Protección de Datos. Con fecha 27/09/2005 D.G.G.G. firmó con la empresa E-Business un contrato de prestación de servicios financieros. Con fecha 24/11/05 ejercitó su derecho de acceso ante E-Business. El 02/12/2005, el reclamante recibió un escrito de la entidad E-Madi Marketing (Arista Marketing, S.L.) con la que no tiene ni ha tenido ninguna relación,

informándole que para darle de baja en sus ficheros era necesario que se comunicará con el número de fax en el que recibió la publicidad. Según informó Arista los datos de D.G.G.G. no figuran en su fichero. Con fechas 12 y 27/12/2006, D.G.G.G. ejercitó de nuevo el derecho de acceso ante la entidad E-Business, la que nuevamente no facilitó el acceso a los datos del reclamante, pese a que se acreditó que E-Business guarda en un fichero en formato papel los datos y documentación de sus clientes y en un fichero informatizado las anotaciones correspondientes a la contratación y, además, solicitó con fecha 16/01/2008 la inscripción del fichero “Análisis y perfiles” en el Registro General de Protección de Datos, que fue inscrito el 22/01/2008. El Director de la Agencia Española de Protección de Datos impone a la entidad E- Business Análisis y Proyectos, S.L., por una infracción del artículo 15.1 de la LOPD, tipificada como grave en el artículo 44.3.e) de dicha norma, una multa de 6.000 euros de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

- RESOLUCIÓN: R/00176/2006. Agencia Española de Protección de Datos. Con fecha 19/11/04 la Agencia Española de Protección de Datos dictó resolución en el procedimiento de tutela de derechos TD/00175/2004, planteado por D.I.G.B., estimando su reclamación e instando a la entidad RELACIONAL para que en el plazo de diez días hábiles siguientes a la notificación de dicha resolución, le remitiese al reclamante certificación en relación con el acceso a los datos existentes en sus ficheros. Con fecha 20/12/04, D.I.G.B. puso de manifiesto ante la Agencia el incumplimiento, por parte de RELACIONAL, de la citada resolución, al haber transcurrido en exceso el plazo establecido de diez días para que le fuera facilitado el acceso a sus datos personales. Con fecha 17/01/05, el Director de la Agencia Española de Protección de Datos dirigió comunicación a RELACIONAL instando nuevamente a la entidad a emitir certificación acreditativa de los datos del denunciante existentes en sus ficheros, sin que ésta atendiera tal requerimiento. El Director de la Agencia Española de Protección de Datos impone a la entidad “RELACIONAL M S.L.”, por una infracción del artículo 15 de la LOPD, tipificada como grave en el artículo 44.3.e) de dicha norma, una multa de 90.000 euros de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.

- RESOLUCIÓN: R/00818/2005. Agencia Española de Protección de Datos. Con fecha 29/11/04, el Director de la Agencia Española de Protección de Datos dictó Resolución R/00516/2004, por la que se ponía fin al procedimiento de Tutela de Derechos TD/00235/2004, y en la que se resolvió estimar la reclamación formulada por D.E.F.A. e instar al Instituto de Gestión Publicitaria, S.L. para que en el plazo de diez días hábiles siguientes a la notificación de la resolución, remitiera al reclamante el acceso completo a sus datos o la certificación de inexistencia de registro alguno relativo a su persona, pudiendo incurrir en su defecto en una de las infracciones previstas en el artículo 44 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las actuaciones realizadas como consecuencia de la resolución deberían ser comunicadas a la Agencia en idéntico plazo de diez días. Sin embargo, la entidad Instituto de Gestión Publicitaria, S.L. no cumplió con la Resolución del Director de la Agencia Española de Protección de Datos. El Director de la Agencia Española de Protección de Datos impone a la entidad por una infracción del artículo 15.1 de la LOPD, tipificada como grave en el artículo 44.3.e) de dicha norma, una multa de 90.000 euros.

- Agencia de Protección de Datos de la Comunidad de Madrid. Tuvo entrada en la Agencia un escrito de la Agencia Española de Protección de Datos, por el cual se remitía la reclamación formulada por D.^a XXXX contra un Hospital de la Comunidad de Madrid, por no haber satisfecho completamente el derecho de acceso a los datos de carácter personal que de ella constaban en el fichero de historias clínicas y en el de usuarios del sistema sanitario de dicho Hospital. En su reclamación, D.^a XXXX ponía de manifiesto que había ejercitado el derecho de acceso y se le había proporcionado parcialmente la información que de ella se contenía en el fichero de usuarios del sistema sanitario del Hospital, constatando además que figuraba cierta información errónea sobre citas de consultas y pruebas médicas que ella no había solicitado y a las que no había asistido. El Hospital presentó escrito de alegaciones en el cual ponía de manifiesto que se habían enviado a la denunciante las fotocopias de los documentos obrantes en su historia clínica y de los datos contenidos en el fichero de usuarios del sistema sanitario, habiendo cumplido por lo tanto con el ejercicio del derecho de acceso de la interesada a sus datos de carácter personal, no vulnerando lo establecido

en el artículo 15 de la LOPD. El Director de la Agencia de Protección de Datos de la Comunidad de Madrid procedió a estimar parcialmente la reclamación formulada por D.ª XXXX, instando al Hospital para que en el plazo de diez días hábiles enviara a la reclamante la información relativa al origen de la recogida de los de los datos personales, las finalidades para las que se habían utilizado y si se habían cedido a terceros, indicando en este supuesto el nombre del cesionario y la finalidad de la cesión, todo ello en relación con los ficheros automatizados de historias clínicas y de usuarios del sistema sanitario.

iv. Infracciones al artículo 16 de la LOPD: derecho de rectificación y cancelación.

- RESOLUCIÓN: R/01370/2009. Agencia Española de Protección de Datos. Con fecha 2 de marzo de 2007, el denunciante remitió un escrito a WKE, S.A., para ejercer su derecho de cancelación ante dicha entidad, solicitando que “se proceda a acordar la cancelación de los datos personales sobre los cuales se ejercita el derecho, y que se realice en el plazo de diez días a contar de la notificación de esta solicitud, rogándoles me notifiquen de forma escrita el resultado de la cancelación practicada”. WKE, S.A., contestó la solicitud de cancelación manifestando que “En contestación a su petición de fecha de 2 de marzo de 2007, le notificamos que se ha procedido a atender su solicitud debidamente”. El 25 de mayo de 2007, el denunciante interpone denuncia en la Agencia, manifestando que ha recibido publicidad postal nominativa a pesar de haber ejercitado su derecho de cancelación. Los datos personales del denunciante resultaron tratados en los sistemas de WKE, S.A. y comunicados a la entidad manipuladora de la impresión de los envíos, a pesar de que el denunciante solicitó la cancelación de los mismos con fecha 2 de marzo de 2007, incluyéndose los siguientes datos personales asociados al denunciante: nombre y apellidos, cargo, dirección, código postal y localidad. El Director de la Agencia Española de Protección de Datos impone a la entidad WOLTERS KLUWE ESPAÑA, S.A., por una infracción del artículo 16 de la LOPD, tipificada como grave en el artículo 44.3 f) de dicha norma, una multa de 60.101,21 euros de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica.

- RESOLUCIÓN R/01292/2009: Agencia Española de Protección de Datos. D.V.V.V. facilitó la dirección de correo electrónico...V.@.... junto con sus datos curriculares a la Bolsa de Empleo de Banesto disponible en Internet en la dirección www....B.....Con fecha 28/03/2007 recibió en la citada dirección dos correos electrónicos enviados por ...B.@.... en cuyo asunto consta “Actualiza tu CV en Banesto”, donde se incluye un código de usuario y una contraseña que permiten acceder a los datos curriculares de un tercero. D.V.V.V. solicitó confirmación de no haber remitido su clave y contraseñas a otra persona. Al no recibir contestación de BANESTO, con fecha 02/04/2007 presentó escrito de solicitud de cancelación de sus datos personales que obraban en su currículum vitae presentado para poder participar en futuros procesos de selección de personal en dicha entidad. Dicha solicitud fue contestada por BANESTO mediante escrito de 24 de abril de 2007 informando del bloqueo de sus datos personales. El 28 de noviembre de 2007, fecha en que se realizó visita de Inspección por la Agencia en BANESTO, se verificó la existencia de información asociada a D.V.V.V. en el fichero “CURRICULUM” sin cancelar o bloquear. El Director de la Agencia Española de Protección de Datos impone a la entidad BANCO ESPAÑOL DE CREDITO S.A., por una infracción del artículo 16.3 de la LOPD, tipificada como grave en el artículo 44.3.f) de dicha norma, una multa de 12.000 euros de conformidad con lo establecido en el artículo 45.2 y 5 de la citada Ley Orgánica.

- RESOLUCIÓN: R/00807/2007. Agencia Española de Protección de Datos. D.J.N.R. solicitó la cancelación de sus datos de los ficheros de la entidad CONSODATA ESPAÑA, S.L.U. (actualmente HERA SERVICIOS TECNICOS AMBIENTALES, S.L.), siendo su solicitud recibida por el responsable del fichero el 21/12/2005. CONSODATA ESPAÑA, S.L.U. comunicó a D.J.N.R. la estimación de su solicitud el 29/12/2005, certificando la cancelación de sus datos. Sin embargo, a finales de diciembre de 2005 ACXION MARKETING SOLUTIONS ESPAÑA, S.A. había obtenido los activos de CONSODATA ESPAÑA, S.L.U. y esta última, vacía de contenido, fue adquirida por HERA SERVICIOS TECNICOS AMBIENTALES, S.L. con la única finalidad de aprovechar la personalidad jurídica de una sociedad ya constituida. En marzo de 2006, D.J.N.R. recibió publicidad de la entidad MBNA EUROPE BANK LIMITES, S.A. en la que figura que los datos utilizados para la referida

campaña provienen de ACXION MARKETING SOLUTIONS ESPAÑA, S.A. El Director de la Agencia Española de Protección de impone a la entidad HERA SERVICIOS TECNICOS AMBIENTALES, S.L., por una infracción del artículo 16.4 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 12.000 euros.

- Agencia de Protección de Datos de la Comunidad de Madrid. Se recibió en la Agencia, la solicitud de tutela del derecho de cancelación presentada por D.XXX contra el Organismo Autónomo YYY, al no haberle dado respuesta alguna dicho Organismo a su solicitud de cancelación de sus datos personales. La Agencia informó al Organismo Autónomo YYY de la reclamación presentada y de la apertura de un procedimiento de tutela de derechos, concediéndole el plazo reglamentariamente previsto para que presentara las alegaciones y pruebas que considerara convenientes. Como respuesta, se recibió escrito del Organismo Autónomo YYY indicando que se procedía al bloqueo de los datos pertenecientes al funcionario, según prevé el artículo 16.3 de la LOPD, por existir causas judiciales abiertas en relación con este funcionario. Intentada la notificación infructuosamente en el lugar indicado por el interesado, se notificó el bloqueo en el domicilio del interesado. En el reglamentario trámite de audiencia previsto para el interesado, éste adujo la nulidad de la aplicación del artículo 16.3 de la LOPD por diversos motivos al considerarlo un bloqueo extemporáneo (producido con posterioridad a los diez días establecidos en la norma), carente de validez jurídica, con vulneración del principio de seguridad jurídica y de la retroactividad de las disposiciones restrictivas de derechos fundamentales, contener disposición imposible, contener restricción de de derechos individuales, vulnerar el principio de igualdad ante la ley, etc. En el posterior trámite de audiencia al Organismo Autónomo YYY, se adujo que se procedió a la cancelación tan pronto como se recibió la solicitud, realizando la notificación en la forma que establece la ley, no produciendo efecto invalidante la notificación fuera de plazo, ya que el RD 1332/1995 regula en su artículo 15 que podrá entenderse desestimada la solicitud no contestada en el plazo previsto, pudiendo entonces el interesado interponer la reclamación correspondiente, por lo que tampoco se produce indefensión. EL Director de la Agencia de Protección de Datos de la Comunidad de Madrid procedió a estimar parcialmente la tutela del derecho de cancelación solicitada por D XXX, puesto que en respuesta al ejercicio de su derecho

de cancelación, el Organismo Autónomo YYY no le comunicó en su momento cancelación alguna. No obstante, puesto que durante la tramitación de este expediente el Organismo Autónomo YYY ha procedido a la cancelación que era posible realizar (bloqueo de los datos por existir abierta causa judicial) no debe hacer ninguna otra actuación de cancelación al respecto.

3.1.2. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución argentina y en la Ley N° 25.326 sobre Protección de Datos Personales.

La protección de la intimidad, de la identidad y en general de los derechos de la personalidad no han estado exentos de evolución en nuestro país vecino, desarrollándose ampliamente doctrina y legislación concordante con las nuevas necesidades de los individuos parte de la República.

Ya en 1994, la Constitución argentina agregó en la Primera Parte del Título Segundo denominado “Nuevas Garantías”, un nuevo artículo 43 que complementó en forma inédita la acción de amparo generalmente conocida. Esta acción, a grandes rasgos, proclama el derecho de toda persona de interponer acción de amparo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesionen, restrinjan, alteren o amenacen, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución, un tratado o una ley.

La reforma constitucional complementó esta garantía general, siguiendo la orientación ya señalada por las nuevas constituciones, con el propósito de jerarquizar el derecho de las personas a conocer y controlar sus propios datos que se hallen registrados en archivos públicos, y privados destinados a proveer informes⁷², planteando la facultad

⁷² GILS CARBÓ, Alejandra, Régimen legal de las bases de datos y hábeas data, Buenos Aires, La Ley, 2001, Pág. 237.

de las personas de sustraerse del flujo incontenible de datos y de la ignorancia de su destino.

En efecto, se agrega en el inciso tercero que:

“Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos”.

Esta acción de amparo protege el derecho a ser informado manifestado en derecho de acceso, modificación, eliminación y bloqueo y se extiende al ejercicio de las siguientes facultades para el afectado:

i. Tomar conocimiento sobre:

- Los datos que consten en registros o bancos de datos públicos.
- Los datos que consten en registros o bancos de datos privados destinados a proveer informes, excluyéndose del ámbito de hábeas data a los archivos de uso personal que son papeles privados⁷³.

ii. Exigir la supresión, rectificación, confidencialidad o actualización de los datos personales que consten en los ficheros ya mencionados, en caso que sean falsos o se verifique discriminación.

⁷³ Los constituyentes optaron por extender la fórmula que había sido utilizada en otros países que sólo contemplaban el habeas data para registros públicos. Asimismo, prefirieron la expresión “bancos de datos privados destinados a proveer informes” a la utilizada en la Constitución Paraguaya que se refiere a “los registros privados de carácter público” lo que a primera vista parece contradictorio, aunque lo que quiere significar es que los registros privados a los que se garantiza acceso son aquellos en los que se registre información que se divulgue al público o sea consultada por terceros.

El hábeas data argentino como expresión de la libertad en una sociedad democrática y tecnológica no declara nuevos derechos ni consagra nuevos principios constitucionales, sino que garantiza a las personas el control sobre sus propios datos y el derecho a ser informado en estas dos modalidades, a través de la provisión de una acción judicial. Además, uno de sus caracteres más importantes radica en posicionarse como un remedio preventivo frente a los daños que se puedan provocar por el mal manejo de la información que le concierne.

La Constitución argentina fue más allá y percibió que los perjuicios derivados de un tratamiento de datos carente de justificación legítima pueden derivar en amenazas de tipo persecutorio o discriminatorio que vulneren diversos bienes jurídicos. Precisamente por esta misma razón, la norma constitucional no dice cuál o cuáles son los bienes jurídicos protegidos por la acción judicial, favoreciendo una amplia aplicación que posibilite la adherencia a criterios más evolucionados que extienden la tutela no sólo a los datos estrictamente íntimos o privados, sino a los que, sin serlo, afecten otros derechos de variada naturaleza, materializándose de una forma más acabada el control sobre los propios datos personales.

En principio, el titular de los datos tiene derecho a conocerlos sólo porque le conciernen, salvo contadas excepciones legales. No obstante, como toda pretensión judicial debe sustentarse en un interés legítimo, de manera que deberá proceder a explicar en su demanda cuáles son los motivos por los que requiere acceder a su registro de datos. Esto no implica que deba acreditar un perjuicio pues precisamente el hábeas data sirve para evitar el daño antes que se produzca.

Además de consagrar el derecho de hábeas data, la legislación argentina incorporó la tutela explícita de la intimidad en el artículo 1.071 bis del Código Civil. También se ha desarrollado un evolucionado derecho a la imagen y al honor a través de los aportes de la jurisprudencia y la doctrina.

Tal es la relevancia que se ha concebido en la República Argentina frente a la protección de datos personales, que también se le ha otorgado tutela legal en el ámbito

provincial, incorporándose normas constitucionales que protegen el derecho a la intimidad en Santiago del Estero, Santa Cruz, Catamarca, Corrientes, Formosa, Neuquén y Salta. Además, provincias como Ciudad Autónoma, Buenos Aires, Córdoba, Chaco, Chubut, La Rioja, San Juan, San Luis, Tierra del Fuego, Jujuy y Río Negro, han incluido al hábeas data como una garantía específica.

Una vez consagrado el recurso de hábeas data a nivel constitucional, comenzaron los intentos de establecer un régimen general de tratamiento de datos personales que recogiera los principios básicos proclamados en otras legislaciones y que armonizará con la iniciativa de la Comunidad Europea de evitar la creación de paraísos informáticos.

Así, los intentos comenzaron con la Ley N°24.745 la que fue vetada en su totalidad por el poder ejecutivo⁷⁴. Luego de esta frustrada iniciativa y el estudio de varios proyectos, se optó por aquel presentado por el Senador Eduardo Menen y que pasó a configurar la Ley N°25.326, la que se estructuró sobre tres pilares fundamentales:

i. La necesidad de ajustarse a los estándares dispuestos por la Directiva 46/95 de la Unión Europea que condiciona la transferencia internacional de datos al cumplimiento de un nivel de protección adecuado y que fijó un plazo de tres años para que los Estados miembros adecuaran sus legislaciones, y otro de cinco para que comenzará a

⁷⁴ Las razones para vetar la Ley N° 24.745 fueron principalmente:

- Era muy estricta en materia de exigencia de consentimiento para la recolección y transmisión de datos a terceros, lo que provocó una fuerte reacción de las corporaciones bancarias, financieras y publicitarias ya que la normativa conduciría a la supresión de la utilización de registros automatizados para proporcionar informes de solvencia y publicidad por marketing directo.
- Instituyó como autoridad de control a una Comisión Bicameral de Seguimiento de Protección Legislativa de datos, que tenía atribuciones amplísimas, incluso de carácter jurisdiccional, vulnerando la separación de poderes del Estado.
- Prohibía la transferencia internacional de datos a países que no estuvieran dotados de una protección adecuada, de manera que se verían afectadas las relaciones y el comercio internacional.
- La acción de hábeas data regulada era insuficiente para una efectiva tutela del afectado ya que no se aplicaba contra órganos públicos.

regir la prohibición de transferencia de datos respecto de países ajenos a esa comunidad. Se percibió que el incumplimiento de estos estándares conllevaba a una inevitable marginación del mercado internacional.

ii. La idea de que las regulaciones sobre tratamiento de datos personales están dispuestas con la finalidad de proteger los derechos de los individuos, es decir, del titular de los datos, a través del establecimiento de obligaciones para los titulares y responsables de los registros.

iii. El reconocimiento de que la reforma constitucional de 1994 no fue suficiente para asegurar un adecuado posicionamiento del hábeas data⁷⁵ en el mundo jurídico argentino. La jurisprudencia de los tribunales tendió a considerar la acción de hábeas data como una simple acción de amparo de carácter excepcional, restrictivo y subsidiario, a lo que se sumó la incertidumbre respecto a los derechos que los titulares podían ejercer en relación a sus datos.

La Ley N° 25.326 sigue muy de cerca el modelo de la Ley Orgánica española de Regulación del Tratamiento Automatizado de Datos, promulgada en 1992 y reformada en 1999 para ajustarse a los estándares fijados por la Unión Europea. Su cuerpo normativo se extiende a regular el tratamiento de datos personales y las reglas procesales necesarias para la aplicación de la acción de amparo de hábeas data.

La legislación argentina, a grandes rasgos, atiende a la exigencia de otorgar un marco legal adecuado al tratamiento de datos personales para el sector público y privado, estableciendo principios sobre calidad de los datos para que éstos sean pertinentes, no excesivos y se obtengan por medios lícitos. Conjuntamente, se distinguen varias categorías de datos, estableciendo el consentimiento del titular cuando corresponda,

⁷⁵ Hubo un fuerte debate en relación a la necesidad de establecer únicamente una reglamentación del hábeas data o un régimen global de tratamiento de datos personales. Aquellos partidarios de reglamentar solamente los aspectos procesales de la ley sostenían que era muy prematuro aventurarse a regular una materia en pleno desarrollo, que ni siquiera Estados Unidos lo había hecho, pues se incrementaban los costos y se obstruían innecesariamente actividades relevantes para el crecimiento de la economía mediante un control excesivo del órgano fiscalizador y del Estado.

imponiendo patrones de seguridad y confidencialidad; y, regulando los derechos de información, acceso, rectificación, actualización o supresión de los datos.

En lo que nos concierne pasaremos a estudiar cómo se consagra el derecho del titular de los datos a ser informado en sus diversas modalidades, a través de la Ley N° 25.326:

1. Derecho a ser informado al recabar datos personales.

Constituye un presupuesto fundamental para que el tratamiento de datos sea legítimo, que el titular de los datos sea informado, extendiéndose ésta información sobre quiénes están procediendo a recolectar los datos y cuál será el destino que se les dará. Así, las personas tendrán oportunidad de decidir –conscientemente- si quieren facilitar a otros la disponibilidad de sus datos personales y con qué alcances⁷⁶.

Este derecho de información se contempla en el artículo 6 de la Ley de Protección de Datos Personales y se manifiesta individual, personalizada y específicamente, ya que se despliega cuando el individuo es requerido acerca de sus datos personales. En este acto, debe informársele en forma expresa y clara acerca de:

- a. La finalidad para la que serán tratados los datos y quienes pueden ser sus destinatarios o clase de destinatarios.
- b. La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable.
- c. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.

⁷⁶ GILS CARBÓ, Alejandra, Régimen legal de las bases de datos y hábeas data, Buenos Aires, La Ley, 2001, Pág. 165.

- d. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.
- e. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de datos.

A través de este detalle, el afectado podrá verificar si el tratamiento de datos se está realizando en conformidad a los principios establecidos en el régimen legal, siendo factible incluso, que requiera el número de inscripción del responsable del registro ante la autoridad de control.

Las precauciones que conlleva el deber de información de este precepto deben acatarse aún con mayor rigor en aquellos casos en los que se exige el consentimiento libre, expreso e informado del titular de los datos. La necesidad de consentimiento será la regla general y no se requerirá consentimiento en los siguientes casos que señala el artículo 5:

- “a) Los datos se obtengan de fuentes de acceso público irrestricto;
- b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
- c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
- d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
- e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley N° 21.526”.

En consecuencia, la recogida de datos personales ya no podrá realizarse descontrolada e invisiblemente, sino que debe promoverse la información mediante

una advertencia clara e inequívoca sobre el destino de los datos obtenidos. Por esta razón, la ley dispone expresamente que si la información figura incluida entre otras declaraciones, debe ubicarse en forma destacada (artículo 5.1), lo que tornaría nulas las cláusulas contenidas en la llamada “letra chiquita” que es típica de los contratos de adhesión, por las que el contratante adherente autorizara la cesión de datos⁷⁷ .

La ley argentina evita distinguir si la información se solicita directamente del titular o de un tercero, siendo forzoso concluir que se refiere a los casos en que la información se recoge del propio titular y no de terceros, atendida la redacción del precepto.

2. El derecho a ser informado manifestado como derecho de acceso.

En la hipótesis que el titular de los datos ha identificado al responsable del fichero y requiera conocer al contenido de este banco de datos, el artículo 14 de la Ley N° 25.326 contempla el derecho de acceso que podrá ejercerse gratuitamente y a intervalos no inferiores a 6 meses, salvo que se acredite un interés legítimo al efecto.

Así se dispone:

“El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes”.

Frente a la solicitud de acceso, el responsable del banco de datos debe proporcionar la información solicitada dentro del plazo de 10 días corridos desde que ha sido intimado fehacientemente. Si vencido este plazo no se ha satisfecho la solicitud o se ha evacuado informe y éste se estima insuficiente, procede ejercer la acción de

⁷⁷ GILS CARBÓ, Alejandra, Régimen legal de las bases de datos y hábeas data, Buenos Aires, La Ley, 2001, Pág. 166 y 167.

protección de datos personales o de hábeas data prevista en el Capítulo VII de la Ley N°25.326.

Como observamos, el derecho de acceso se traduce en la acción de hábeas data, presentándose de variadas formas, como un reclamo entre particulares si se trata de un registro de titularidad privada, por vía administrativa si el registro es público o a través de la acción judicial propiamente tal. El objeto de su ejercicio consiste en tomar conocimiento sobre el contenido de los datos personales.

El procedimiento de acceso, se desarrolla en su primera etapa, con la petición del titular de los datos al responsable del registro, previa acreditación de su identidad⁷⁸. Los registros deberán establecer sus estructuras y su organización, de manera de hacerla compatible con el ejercicio del derecho de acceso. Esta petición podrá realizarse verbalmente, sin embargo, para ejercer la acción de hábeas data, el titular deberá hacer constar que ya solicitó acceso a sus datos y su solicitud no se ha satisfecho o el informe fue insuficiente, siendo más conveniente ejercer el derecho por un medio fehaciente.

Una vez que el titular de los datos ha solicitado acceso, el responsable del fichero deberá producir un informe en el plazo de 10 días⁷⁹, contestando en forma clara y en lenguaje accesible al conocimiento medio de la población, de forma decodificada, valiéndose de una explicación que facilite la comprensión si fuere necesario. Además, la contestación deberá ser amplia y versar sobre la totalidad del registro, aún cuando el requerimiento contemple sólo una parte de los datos personales.

⁷⁸ La Ley de Protección de Datos Personales argentina amplía de manera expresa la legitimación del solicitante, posibilitándose el ejercicio del derecho de acceso a los sucesores universales de las personas fallecidas y a los apoderados o representantes legales del afectado.

⁷⁹ "Gutiérrez, Vicente Juan Carlos Demetrio con Banco de la Provincia de Buenos Aires y otro". C.N. Civ., Sala K, 22/10/02. "Toda empresa de verificación de riesgos crediticios debe, ante una intimación requiriendo información sobre datos personales inexactos y/o falsos referidos a una calificación personal, actuar con la -mayor celeridad posible utilizando todos los medios que se encuentren a su disposición tales como el "Fax", e-mail o cualquier otro tipo de procedimiento electrónico que permita obtener la información precisa de inmediato y sin tener que esperar un plazo prolongado. Una actitud contraria a la descripta, denota un obrar negligente o descuidado frente al interés concreto y fundamentado del particular, susceptible de producir responsabilidad

Argentina cuenta con jurisprudencia importante respecto al ejercicio del hábeas data y el establecimiento de éste como herramienta de protección de los derechos individuales. La primera vez, que la Corte Suprema de Justicia de la Nación Argentina se pronunció sobre el hábeas data fue en el caso “Urteaga, Facundo Raúl con Estado Mayor Conjunto de las FF. AA.”, sentando las bases para el éxito de la acción.

En este caso, el demandante dedujo acción de hábeas data con el objeto de obtener información respecto al destino de los restos de su hermano -quién se suponía fallecido en una acción militar el año 1976- los motivos de su desaparición, los responsables y el grado de responsabilidad que se le atribuía al Estado. Para el cumplimiento de estos fines, la acción de hábeas data tenía por objeto requerir de información a:

- Bancos de datos de la Secretaría de Informaciones del Estado.
- Servicio de Inteligencia de Aeronáutica.
- Servicio de Inteligencia de la Policía Federal.
- Servicio de Informaciones de la Policía de la Provincia de Buenos Aires.
- Servicio de Inteligencia de la Provincia de Buenos Aires.
- Y/o Cualquier otro banco de datos del Estado Nacional y las Fuerzas Armadas.

La demanda de Urteaga había sido rechazada totalmente en primera y segunda instancia. Sin embargo, la Corte Suprema de Justicia de la Nación revocó parcialmente la decisión, declarando la amplitud de los alcances del hábeas data, “tanto en lo relativo a la exigencia de licitud, lealtad y exactitud en la información, como en lo que hace al acceso de las personas legitimadas”. Se consideró que las causales de excepción no procedían y el actor tenía derecho a obtener “la información objetiva requerida, para lo cual deberá disponer el libramiento de los oficios necesarios a fin de

que los organismos requeridos den cuenta si en sus registros obra constancia del fallecimiento de Benito José Urteaga y, en su caso, la localización de sus restos⁸⁰.

3. Derecho a ser informado manifestado como facultad de solicitar información al organismo de control.

El artículo 13 de Ley N°25.326 señala:

“Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El registro que se lleve al efecto será de consulta pública y gratuita”.

Esta fase del derecho de información se refiere a la facultad del titular de los datos de consultar y conocer, en forma gratuita, los siguientes puntos:

- Los archivos, registros o bases de datos existentes.
- La finalidad de los archivos, registros o bases de datos existentes.
- La identidad de los responsables de los archivos, registros o bases de datos existentes.

Por lo tanto, el derecho de consulta abarca sólo aspectos básicos de los archivos que se encuentran inscritos, para que los individuos que tiene razones para recelar sobre determinado tratamiento de datos y una eventual vulneración de derechos puedan comenzar a indagar sobre quiénes están tratando su información. Quedan fuera del ámbito de consulta lo concerniente al procedimiento de recolección de datos, la estructura del archivo, las medidas de seguridad, las cesiones y las clases de datos que contiene el registro.

⁸⁰ S. C. U. 14, L. XXXIII, sentencia del 15 de octubre de 1998.

4. Derecho a ser informado manifestado como derecho de rectificación, actualización, integración, bloqueo o supresión.

Como ya señalamos, la Constitución Nacional de la República Argentina consagró en su modificación de 1994, el derecho de supresión, rectificación, confidencialidad o actualización, en caso de falsedad o discriminación, de los datos personales que consten en registros o bancos de datos. Este catálogo de derechos se vio reforzado con la dictación de la Ley N° 25.326, dando lugar a los siguientes derechos para el afectado:

i. Rectificar los datos falsos, erróneos o inexactos (artículos 4.4, 4.5 y 16). Procederá suprimirlos cuando no pueda establecerse la veracidad de la información.

ii. Suprimir los datos inadecuados, impertinentes o excesivos según los principios de calidad y sujeción al fin del registro que trascienden la ley (artículos 4.1 y 4.3) y particularmente en los casos que la recogida:

- Estuviere prohibida, como es el caso del artículo 7 de los datos sensibles.
- Se hubiere realizado por medios desleales, fraudulentos o contrariamente a las disposiciones de la ley, de acuerdo a lo preceptuado por el artículo 4.2.
- Se hubiere realizado sin el consentimiento libre, expreso e informado del afectado como disponen los artículos 5 y 11.

iii. Requerir la supresión de los datos caducos o que hubieran devenido en innecesarios de acuerdo a lo dispuesto en el artículo 4.7. En estos casos se deberá proceder a la supresión porque el interés legítimo en conservar los datos se ha desvanecido y la difusión de un dato obsoleto puede configurar un abuso del derecho a informar sancionado por el artículo 1.701 del Código Civil argentino.

Además se contemplan casos específicos en que procede el derecho a requerir supresión:

- Supresión de datos para publicidad (artículo 27.3).
- Supresión de datos sobre información crediticia transcurridos dos o cinco años según corresponda (artículo 26.4).
- Supresión de datos personales registrados con fines policiales cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento (artículo 23.3).

iv. Exigir la confidencialidad de los datos potencialmente dañosos. Cualquier acto, conducta o sentimiento que la persona titular de los datos desee calificar de reservado, preservándolo del conocimiento externo, deviene en un deber de secreto para el titular del fichero. Si éste tiene derecho a conservarlo deberá bloquear el dato⁸¹ para impedir el acceso a terceros. La cancelación no podrá efectuarse cuando pudiera provocar perjuicios a intereses legítimos del afectado, de terceros o cuando existiese una obligación de conservar los datos, como señala el artículo 16.5.

v. Actualizar los datos obsoletos o vetustos de acuerdo a lo dispuesto en el artículo 4.4. cuando el reajuste de los datos sea relevante para el titular por afectar un interés legítimo y jurídicamente protegido.

vi. Integrar o adicionar información que estuviera incompleta. Se considera que el dato está incompleto cuando la omisión de algún aspecto del dato modifica de manera importante el sentido de la información. Esta hipótesis no está de forma expresa en la ley pero puede asimilarse con la inexactitud y el error.

El artículo 16.2 señala que una vez que el responsable o usuario del banco de datos ha recibido la solicitud de rectificación, supresión, bloqueo, actualización o integración tiene 5 días hábiles para dar cumplimiento al requerimiento de titular de los datos. El plazo también es de 5 días hábiles si es el responsable o usuario de banco de datos quien ha advertido el error o falsedad.

⁸¹ La Ley de Protección de Datos Personales, se refiere al bloqueo como solución provisional que puede adoptar el responsable del archivo o el juez mientras se desarrolle el proceso de verificación del dato, si estima que es manifiesto el carácter discriminatorio, falso o inexacto (artículo 16 .6 y artículo 38.4).

Mientras se proceda a examinar la procedencia de la solicitud, el responsable o usuario del banco de datos debe bloquear el archivo cuestionado o consignar que está sujeto a revisión, tal como señala el artículo 16.6.

Si el responsable o usuario del banco de datos no responde a la solicitud del afectado o el informe se considera insuficiente, procede la interposición de acción de hábeas data.

Si los datos corregidos fueron transmitidos, cedidos o transferidos a un tercero, el responsable o usuario del banco de datos deberá notificar la corrección, rectificación, supresión o acto similar al tercero, dentro del quinto día hábil desde que se efectuó el tratamiento (artículo 16.4).

La acción de hábeas data que contempla la Ley N° 25.326 en los artículos 33 y siguientes, se ejerce ante el juez del domicilio del demandado. La competencia federal procede cuando se interponga contra archivos públicos de organismos nacionales y cuando los archivos de datos se encuentren interconectados en redes jurisdiccionales, nacionales o internacionales.

No se establece un recurso frente a la denegación de la solicitud frente al organismo de control, sólo se señala que el organismo de control deberá llevar un registro y que en caso de rechazo de la acción, ésta no constituye presunción de responsabilidad en que hubiera podido incurrir el demandante.

Limitaciones al derecho a ser informado en sus distintas manifestaciones.

Como señala la Corte Suprema de Justicia de la Nación, los derechos declarados por la Constitución Nacional no son absolutos, y entre ellos, el derecho de acceso a los datos personales cede ante la necesidad de preservar otros intereses públicos o privados.

De acuerdo al artículo 17 de la Ley N° 25.326, los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de:

- La defensa de la Nación.
- El orden y la seguridad públicos.
- La protección de los derechos e intereses de terceros.

La información sobre datos personales también podrá ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre:

- El cumplimiento de obligaciones tributarias o previsionales.
- El desarrollo de funciones de control de la salud y del medio ambiente.
- Delitos penales.
- La verificación de infracciones administrativas.

La resolución que así lo disponga debe ser fundada y notificada al afectado. Sin perjuicio de lo señalado, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

La palabra decisiva la tendrán los jueces, quienes deberán determinar el adecuado equilibrio entre la protección de funciones que son esenciales para el Estado y los derechos de los particulares, teniendo siempre en cuenta que la interpretación tendrá que ser limitada a casos excepcionales y debidamente fundados.

Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.

La Unión Europea, a través de la Directiva 95/46 impuso a los Estados Miembros, instituir una autoridad de control, capaz de fiscalizar el cumplimiento de la ley, dotada

de amplias facultades de investigación e intervención que le permitan, incluso, ordenar el bloqueo, supresión o destrucción de los datos tratados ilegítimamente.

Argentina percibió que la creación de un organismo administrativo de control cumple un rol fundamental porque se posibilita que la tutela adecuada se estructure sobre la base de la prevención, antes que los daños se produzcan. Así, la Ley N° 25.326 creó una autoridad de control a semejanza de las legislaciones europeas, el Director, que es un órgano unipersonal, designado por el Poder Ejecutivo y que dura en su cargo cuatro años.

El Director tendrá diferentes facultades vinculadas al cumplimiento de la obligación de informar y a la sanción de su incumplimiento:

- i. Asistencia y asesoramiento: el Director debe asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y los medios legales de que disponen para la defensa de los derechos que la ley garantiza. Este deber de asesoramiento puede operar también en beneficio de los responsables de los registros para ser aconsejados sobre puntos dudosos.
- ii. Normativas: el Director debe dictar las normas y reglamentaciones que se deben observar en el desarrollo de actividades comprendidas en esta ley, estableciendo pautas generales para todos los registros que deberán graduarse en función de la naturaleza de los datos y de la actividad que realiza el registro.
- iii. Registrales: el Director debe efectuar un censo de archivos, registros o bancos de datos alcanzados por ley, manteniendo un registro permanente de éstos. En el marco de esta facultad, deberá controlar el cumplimiento de los requisitos y garantías que deben reunir los bancos de datos.
- iv. Inspección e investigación: el Director tiene la facultad de inspeccionar e investigar para controlar el cumplimiento de las normas, en especial en lo relativo al cumplimiento de las normas sobre integridad y seguridad.

v. Disciplinarias: esta facultad se posiciona como la de mayor relevancia en el cargo de Director porque otorga la potestad de controlar el acatamiento de la ley por vía compulsiva y represiva, imponiendo las sanciones administrativas que correspondan por la vulneración de las normas sobre protección de datos personales. De esta forma se genera una mayor política preventiva.

Una vez que el Director verifica la infracción a la ley procederá a imponer sanciones, tomando en cuenta el marco general que le otorga el artículo 31 de la Ley N° 25.326, las que operaran sin perjuicio de las responsabilidades administrativas que se derivan de los bancos de datos públicos, de la responsabilidad por daños y perjuicios consecuencia de la inobservancia de la ley y de las sanciones penales que correspondan:

“El organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos a cien mil pesos⁸², clausura o cancelación del archivo, registro o banco de datos”.

Las condiciones y procedimientos para aplicar las sanciones previstas, son fijadas mediante reglamentación al efecto. Las sanciones deberán graduarse en relación a la gravedad y extensión de la violación de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. La ley no hace una tipificación específica acerca de la conducta sujeta a infracción, disponiendo sólo de un marco por el cual deberá regirse.

En consecuencia, la sanción al incumplimiento de derecho a ser informado, los estándares aplicados y la reglamentación al efecto, dependerán intrínsecamente de la labor ejercida por el Director, pues la Ley N° 25.326 sólo otorga una base general desde la cual deberá sustentarse el sistema de penas.

⁸² Desde \$134.467 a \$13.446.707 según conversión de moneda calculada de acuerdo a promedio correspondiente a marzo de 2010.

Precisamente, en virtud de las atribuciones asignadas al Director Nacional de Protección de Datos Personales, especialmente en lo relativo a la facultad de imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la Ley N° 25.326 y de las reglamentaciones dictadas en su consecuencia, se dicta la Disposición N° 7/2005, en la cual se aprueba la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante violaciones a las normas de la Ley N° 25.326 y de las reglamentaciones dictadas en su consecuencia.

Así, se establece:

i. Serán consideradas infracciones leves, sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos también las constituyan:

- No atender la solicitud de acceso, rectificación o supresión de los datos personales objeto de tratamiento cuando legalmente proceda.
- No proporcionar la información que solicite la Dirección Nacional de Protección de Datos en el ejercicio de las competencias que tiene atribuidas.
- No solicitar la inscripción de las bases de datos personales tanto públicas como privadas cuyo registro sea obligatorio en los términos exigidos por la Ley N° 25.326 y normas complementarias.
- Recoger datos de carácter personal sin proporcionar a los titulares de los mismos la información que señala el artículo 6 de Ley N° 25.326 o sin recabar su consentimiento libre, expreso e informado en los casos en que ello sea exigible.
- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido por el titular. Entiéndase incluida en este supuesto la negativa a retirar o bloquear el nombre y dirección de correo electrónico de los bancos de datos

destinados a publicidad cuando su titular lo solicite de conformidad con lo previsto en el último párrafo del artículo 27 de la Ley N° 25.326.

- Proceder al tratamiento de datos de carácter personal que no reúnan las calidades de ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

ii. Serán consideradas infracciones graves, sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos Personales también las constituyan:

- Tratar los datos de carácter personal en forma ilegítima o con menosprecio de los principios y garantías establecidos en Ley N° 25.326 y normas reglamentarias.

- Realizar acciones concretas tendientes a impedir u obstaculizar el ejercicio por parte del titular de los datos del derecho de acceso o negarse a facilitarle la información que sea solicitada.

- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones, actualizaciones o supresiones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la Ley N° 25.326 ampara y haya sido intimado previamente por la Dirección Nacional de Protección de Datos Personales.

- Obstruir el ejercicio de la función de inspección y fiscalización a cargo de la Dirección Nacional de Protección de Datos Personales.

- No inscribir la base de datos de carácter personal en el registro correspondiente, cuando haya sido requerido para ello por la Dirección Nacional de Protección de Datos Personales.

- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por la Dirección Nacional de Protección de Datos Personales.

- Recoger datos de carácter personal mediante ardid o engaño.

- iii. Serán consideradas infracciones muy graves, sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos Personales también las constituyan:
 - Conformar un archivo de datos cuya finalidad sea contraria a las leyes o a la moral pública.

 - Transferir datos personales de cualquier tipo a países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, salvo las excepciones legales previstas en el artículo 12, inciso 2, de la Ley N° 25.326, sin haber cumplido los demás recaudos legales previstos en la citada ley y su reglamentación.

 - Ceder ilegítimamente los datos de carácter personal fuera de los casos en que tal accionar esté permitido.

 - Recolectar y tratar los datos sensibles sin que medien razones de interés general autorizadas por ley o tratarlos con finalidades estadísticas o científicas sin hacerlo en forma disociada.

 - Formar archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, salvo en los casos expresamente previstos en el artículo 7º, inciso 3), de la Ley N° 25.326.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías reconocidos en nuestra Carta Magna, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales⁸³.

La disposición 7/2005 establece que las infracciones generan la imposición de sanciones monetarias, fluctuando en los siguientes valores:

- Ante la comisión de infracciones leves se podrán aplicar hasta dos apercibimientos y/o una multa de 1.000 a 3.000 pesos, es decir, alrededor de \$134.533 a \$403.601 pesos chilenos⁸⁴.
- Ante la comisión de infracciones graves se podrán aplicar hasta cuatro apercibimientos, suspensión de uno a treinta días y/o multa de 3.001 a 50.000 pesos, es decir, alrededor de \$403.734 a \$6.726.660.
- Ante la comisión de infracciones muy graves se podrán aplicar hasta seis apercibimientos, suspensión de treinta y un o a trescientos sesenta y cinco días, clausura o cancelación del archivo, registro o banco de datos y/o multa de 50.001 a 100.000 pesos, es decir, alrededor de \$6.726.795 a \$13.453.211.

La legislación argentina también ha incluido sanciones penales para las conductas que infrinjan los deberes y obligaciones contemplados en la Ley N° 25.326, agregándolas en los artículos 117 bis y 157 bis del Código Penal. Sin embargo, ninguna de estas sanciones está dirigida al incumplimiento del derecho a ser informado en sus distintas modalidades.

⁸³ La disposición 7/2005 establece un catálogo de infracciones más amplio, aquí sólo se hace referencia a las que se vinculan, directa o indirectamente, al derecho a ser informado en sus diferentes manifestaciones.

⁸⁴ Conversión de moneda calculada según promedio correspondiente a marzo de 2010.

3.1.3. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución colombiana y en la Ley Estatutaria 1.266.

La Defensoría del Pueblo Colombiano, en el ejercicio de su tarea de impulsar la efectividad de los derechos humanos en el marco de un Estado social de derecho, democrático, participativo y pluralista, ha discutido ampliamente la necesidad y las características de la regulación legal del hábeas data.

Ya en a principios de la década de los noventa, está preocupación hizo eco con la promulgación de la Constitución de 1991 que incluyó en el artículo 15 sobre el derecho a la intimidad e inviolabilidad de las comunicaciones privadas, el derecho de las personas a:

“conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”.

El problema radica en que a pesar de la previsión constitucional, no fue posible que la ciudadanía contara con una legislación que protegiera los datos de carácter personal y estableciera las condiciones de legalidad para la operación de bases de datos de carácter público y privado.

Frente a la carencia de una ley específica, la protección del derecho de hábeas data estuvo a cargo de la Corte Constitucional Colombiana mediante la acción de tutela, constituyéndose uno de los avances jurisprudenciales más significativos del derecho de protección de datos en América Latina. A través de un centenar de fallos se estableció el carácter autónomo de este derecho y las reglas que lo gobiernan.

Pese a este avance, se percibió que era imprescindible legislar en concreto para la protección de los datos personales, estableciendo una protección que opere preventivamente y cuyos alcances sean generales. Incluso, a través de la sentencia T-729 de fecha 5 de septiembre de 2002, la misma Corte Constitucional Colombiana exhorto al Procurador General de la Nación y al Defensor del Pueblo para que en el ejercicio de sus deberes constitucionales promovieran la presentación de un Proyecto de Ley Estatutaria. Asimismo, se llamó al Congreso de la República para que tramitara y aprobara el respectivo proyecto sobre las condiciones de ejercicio, principios y mecanismos judiciales y administrativos de protección de los derechos fundamentales a la autodeterminación informativa, hábeas data, intimidad, libertad e información, entre otros.

De los títulos de los Proyectos de Ley Estatutaria presentados al Congreso, el 64% de éstos optaron por un enfoque integral, mientras que el 36% restante obedeció a proyectos que pretendían regular el hábeas data pero únicamente respecto de la información comercial o financiera⁸⁵. Finalmente, se optó por Proyectos de Ley Estatutaria de carácter general que desarrollaran el texto constitucional que reconoce y garantiza el derecho a controlar la información personal que le concierne a los individuos.

Para el cumplimiento de estos fines, en junio de 2007 el Congreso de la República de Colombia aprobó el Proyecto de Ley Estatutaria 221 de 2007 del Senado. Luego, de acuerdo a lo establecido en el artículo 153 de la Constitución Colombiana, la Corte Constitucional realizó la revisión previa necesaria para declarar la asequibilidad del proyecto. Ocurrido esto, se dictó la Ley Estatutaria 1.266 del 31 de diciembre de 2008, mediante la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

⁸⁵ DEFENSORÍA DEL PUEBLO COLOMBIANO, Memorias del foro sobre Protección de datos Personales y Regulación Legal del Hábeas Data, Dirección Nacional de Promoción y Divulgación de Derechos Humanos, Bogotá, 2004, Pág. 54.

A diferencia de la legislación española y argentina, ya estudiadas, que establecen las obligaciones y deberes en los responsables de los bancos de datos, la Ley Estatutaria 1.266 realiza tres distinciones entre la fuente de información, el operador de la información y el usuario.

i. Fuente de información:

- Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de un servicio o de cualquier otra índole.
- En razón de la autorización legal o del titular, la fuente de información suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.
- Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá simultáneamente la condición de fuente y operador y asumirá los deberes y responsabilidades de ambos.
- La fuente de la información da cuenta de la calidad de los datos suministrados al operador y al acceder y suministrar información personal de terceros, debe cumplir los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.

ii. Operador de información.

- Es la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros que establece la ley.

- Al acceder a información personal de terceros, debe cumplir los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos.

- Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

iii. Usuario.

- El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información.

- El usuario, al acceder a información personal de terceros, debe cumplir los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos.

- En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

Esta distinción es de fundamental importancia, ya que la Ley Estatutaria 1.266 establece obligaciones según el rol que ejerza la entidad pública o privada en el tratamiento de datos personales, distinguiendo si estamos ante una fuente de información, un operador de información o un usuario de información.

En cuanto al derecho a ser informado que detenta el titular del fichero este se desarrollará de una manera distinta dependiendo del tipo de información, del órgano y la etapa de tratamiento:

1. Derecho a ser informado en el tratamiento general de datos personales.

i. Derecho a ser informado por la fuente de información.

De acuerdo a la definición de fuente de información, esta sería la primera persona, entidad u organización que accede a los datos personales, de manera que parecería lógico que se le atribuyera la obligación de informar al titular de los datos, previamente a la solicitud, sobre la existencia del registro, la identidad del titular del banco de datos, su domicilio, la finalidad de la recogida, los destinatarios de la información, el carácter obligatorio o facultativo de la entrega de datos, los derechos que le asisten, entre otros.

Sin embargo, la Ley Estatutaria impone diversos deberes de información, prescindiendo de la obligación estricta de informar al recoger los datos personales:

- Debe informarse al titular sobre la finalidad de la recogida de datos previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto (artículo 4 letra b).
- Frente a la fuente de información pueden ejercerse los derechos fundamentales al hábeas data y de petición (conocer, actualizar y rectificar) pero su cumplimiento se realizará a través de los operadores, con base en la información aportada por la fuente, conforme lo previsto en los procedimientos de consultas y reclamos (artículo 6 derecho 2.1).
- Frente a la fuente puede solicitarse información o pedir la actualización o rectificación de los datos contenidos en el registro, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones (artículo 6 derecho 2.2).

En este sentido, la fuente debe garantizar que la información que se suministra a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable (artículo 8.1).

- Frente a la fuente puede solicitarse prueba de la autorización⁸⁶, cuando dicha autorización sea requerida conforme a la ley (artículo 6 derecho 2.3). Es deber de la fuente solicitar y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, asegurándose de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado (artículo 8.5).

ii. Derecho a ser informado por los operadores de los bancos de datos.

Como señalamos el operador de bancos de datos es la persona, entidad u organización que se posiciona como un intermediario entre la fuente de información y el usuario, ejerciendo una función de administración y de comunicación de datos. Como el operador no ha realizado la recogida de datos, salvo que ejerza simultáneamente el rol de fuente y operador, no le corresponde interactuar con el titular y solicitarle la autorización para la recogida de datos, ni informarle la finalidad que reside en el tratamiento. Tampoco se hace responsable de la calidad de los datos, pero debe garantizar y propender a la protección de los derechos del titular de los datos.

La Ley Estatutaria señala que frente a los operadores de bancos de datos se puede:

⁸⁶ De acuerdo a la Ley Estatutaria Colombiana la administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la ley.

La administración de datos semi-privados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En todo caso, la administración de datos semi-privados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de Ley.

- Ejercer el derecho de hábeas data (conocer, actualizar y rectificar) en los términos que señala la ley, a través de los procedimientos de consultas y reclamos, sin perjuicio de los demás mecanismos constitucionales y legales (artículo 6 derecho 1.1). Cuando se determinada información se encuentre en discusión, el operador deberá indicar en el registro que el dato está en procedimiento de impugnación (artículo 7.9).
- Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario (artículo 6 derecho 1.3).
- Solicitar información acerca de los usuarios autorizados para obtener la información (artículo 6 derecho 1.4).

iii. Derecho a ser informado por los usuarios.

Como señalamos el usuario constituye el último eslabón de la cadena de utilización del tratamiento de datos personales, en el sentido que accede a la información que la fuente le ha suministrado al operador. Si el usuario utiliza información que el mismo ha recogido del titular de los datos, será simultáneamente fuente y usuario.

Los derechos que pueden hacerse valer frente al usuario son:

- Solicitar información acerca de la utilización que el usuario le está dando a la información (artículo 6 derecho 3.1 y artículo 9.2).
- Solicitar prueba de la autorización, cuando ella haya sido requerida conforme lo previsto en la presente ley.

2. Derecho a ser informado en el tratamiento de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

A diferencia del régimen general en el tratamiento de datos personales, el título IV de la Ley Estatutaria colombiana establece un régimen especial para los bancos de datos

de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

De acuerdo al principio de favorecimiento a una actividad de interés público, este tipo de información promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo. Por lo tanto, la administración de esta información por parte de las fuentes, usuarios y operadores deberá realizarse de forma que permita favorecer los fines de expansión y democratización del crédito.

Los usuarios de la información deberán valorar estos datos en forma concurrente con otros factores o elementos de juicios que técnicamente inciden en el estudio de riesgo y en el análisis crediticio, y no podrán apoyarse únicamente en la información relativa al incumplimiento de obligaciones proporcionada por los operadores para tomar decisiones frente a solicitudes de crédito⁸⁷. Si los usuarios de la información niegan una solicitud de crédito basados exclusivamente en la información negativa del solicitante, la Superintendencia de Financiera de Colombia podrá imponer las sanciones legales que correspondan.

Así, se permitirá valorar la información financiera positiva de las personas, facultándose a los operadores de información para mantenerla de forma permanente y e indefinida en sus bancos de datos, a fin de utilizara en decisiones frente a solicitudes de crédito. El régimen es distinto en la información negativa cuya permanencia será de cuatro años contados desde la fecha en que sea pagada la obligación vencida.

El tratamiento de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países por parte de los operadores se condiciona al cumplimiento de variados requisitos especiales estipulados en el artículo 11 de la ley:

⁸⁷ El artículo 14 párrafo 4 de la Ley Estatutaria 1.266 prohíbe la administración de datos personales con información exclusivamente desfavorable.

- a) La constitución del operador como sociedad comercial, entidad sin ánimo de lucro o entidad cooperativa.
- b) El establecimiento de un área de servicio al titular de información, para la atención de peticiones, consultas y reclamos.
- c) La instauración de un sistema de seguridad y condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme a lo previsto en la misma ley.
- d) El operador deberá actualizar la información reportada por las fuentes con una periodicidad no superior a diez días calendario contados desde el recibo de la misma.

En lo que respecta a las fuentes de información, estas deberán cumplir las siguientes prescripciones legales:

- a) Actualizar mensualmente la información suministrada al operador.
- b) Comunicar al titular de la información la realización y el contenido del reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
 - El objetivo de la comunicación al titular consiste en que este pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y la fecha de exigibilidad. La comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes.
 - La fuente de información podrá proceder a evacuar el reporte de la información transcurridos veinte días calendarios siguientes a la fecha de envío de la comunicación en la última dirección de domicilio del afectado que se encuentre registrada en los

archivos de la fuente de información. Si la información se encuentra en discusión, este aspecto debe ser informado al operador.

Así, el derecho del titular de los datos a ser informado, se manifiesta de la siguiente forma:

1. Frente a la fuente de información. Derecho a ser informado previamente a la remisión del reporte de información financiera, crediticia, comercial, de servicios y proveniente de terceros países, de carácter negativo al operador de información. La notificación podrá realizarse a través de los extractos periódicos enviados al domicilio del cliente (artículo 12 inciso 2 y 3).

2. Frente al operador. Derecho a ser informado manifestado como derecho de consulta a la información personal que repose en el banco de datos, sea del sector público o privado. El operador deberá suministrar al solicitante toda la información contenida en el registro individual o que esté vinculada con la identificación del titular. La petición de consulta podrá realizarse de forma verbal, escrita o por cualquier canal de comunicación, procurando mantener evidencia por medios técnicos, ya que una vez recibida la petición el operador deberá evacuar una respuesta en el plazo de diez días hábiles.

3. Frente al operador. Derecho a ser informado manifestado como derecho a solicitar corrección o actualización. Si una vez consultada la información, el titular verifica una anomalía, podrá presentar un reclamo para que la información sea enmendada o ajustada al presente.

En cuanto a los derechos de información contemplados por la legislación colombiana, estos no difieren de forma rotunda entre el régimen general y el régimen previsto para información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Los derechos individualizados en los números 2 y 3 recién estudiados se contemplan de forma generalizada, sin embargo, el derecho a notificar al afectado sobre el reporte de información financiera es un derecho exclusivo para este tipo de

datos y es una innovación de fundamental importancia si la comparamos con otras legislaciones.

De acuerdo al procedimiento de consultas y reclamos dispuesto para todos los bancos de datos y todos los tipos de información, se establece en el artículo 16.6. que sin perjuicio del ejercicio de la acción de tutela para amparar el derecho de hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta otorgada a su petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida, demanda que deberá interponerse contra la fuente de información.

Llama la atención que este derecho a interponer acción legal contra la fuente de información, se contenga en el Título V de consultas y reclamos dispuesto para todos los tipos de información, cuando realmente el derecho a accionar contra la fuente de información se fundamentaría en “la obligación reportada como incumplida”, datos que pertenecen a la categoría de económicos y no “cualquier dato”.

Incumplimiento de la obligación de informar al titular de los datos personales en sus distintas modalidades.

Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del Hábeas Data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición de información, consulta, acceso, corrección y actualización podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida.

Esta demanda deberá ser interpuesta contra la fuente de información, la que una vez notificada de la demanda procederá a informar al operador dentro de los dos días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro del registro individual, lo cual deberá hacer el operador dentro de los dos días

hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo firme.

En cuanto a la vigilancia frente a los incumplimientos de los destinatarios de la ley, ésta ha quedado radicada en un órgano de control. Cuando la Defensoría del Pueblo colombiano proyectó como debería posicionarse una autoridad de control y vigilancia, señaló:

“Para su creación en Colombia, se debería considerar la experiencia extranjera en la materia. Particularmente, y con miras a no repetir los errores que se han dado en otros países, es necesario tener presente que la falta de recursos y de independencia son los dos principales problemas detectados internacionalmente. En cuanto a la falta de independencia, recientemente el *Electronic Privacy Information Center* (EPIC) destacó casos como Tailandia, en donde la autoridad de control depende de la oficina del Primer Ministro. Luego de un desacuerdo entre estos dos, el director de la autoridad de control fue removido de su cargo⁸⁸”.

La Ley Estatutaria 1.266 radica las facultades de vigilancia y control en la Superintendencia de Industria y Comercio⁸⁹ que ejercerá sus funciones frente a los operadores, las fuentes de información y los usuarios de información financiera,

⁸⁸ DEFENSORÍA DEL PUEBLO COLOMBIANO, Memorias del foro sobre Protección de datos Personales y Regulación Legal del Hábeas Data, Dirección Nacional de Promoción y Divulgación de Derechos Humanos, Bogotá, 2004, Pág. 65.

⁸⁹ Si la vigilancia de la fuente u operador de información le corresponde a la Superintendencia Financiera de Colombia, será ésta quién ejerza las funciones e imponga las sanciones correspondientes, de conformidad a las facultades que le son propias, de acuerdo a lo establecido en el Estatuto Orgánico del Sistema Financiero y las demás normas pertinentes.

crediticia, comercial, de servicios y la proveniente de terceros países, otorgándosele las siguientes facultades:

i. Instructivas: podrá impartir instrucciones y órdenes sobre la manera de cumplir las disposiciones de la ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, fijando los criterios que faciliten el cumplimiento y los procedimientos para su íntegra aplicación.

ii. Garantistas:

- Debe velar por el cumplimiento de las disposiciones de la ley, de las normas que la reglamenten y de las instrucciones impartidas por la Superintendencia.

- Deberá cautelar que los operadores y fuentes cuenten con un sistema de seguridad y condiciones técnicas adecuadas.

- Para el cumplimiento de estas tareas podrá ordenar auditorías externas para verificar el cumplimiento de las disposiciones.

- Podrá ordenar de oficio o a petición de parte⁹⁰ la corrección, actualización o retiro de los datos personales cuando ello sea procedente, conforme a lo establecido en la ley.

iii. Investigativas: podrá iniciar de oficio o a petición de parte investigaciones administrativas contra operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones o de las órdenes o instrucciones impartidas por el organismo de vigilancia respectivo, y si es el caso imponer sanciones u ordenar medidas pertinentes.

⁹⁰ Previa acreditación ante la Superintendencia que se realizó el trámite de reclamo por los mismos hechos ante el operador, y que éste no fue atendido o fue atendido desfavorablemente.

iv. Sancionatorias: podrá imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, previas explicaciones de acuerdo al procedimiento aplicable, multas, suspensiones y clausura de las operaciones del banco de datos.

Cabe señalar que las facultades sancionatorias de la Superintendencia de Industria y Comercio y la Superintendencia Financiera tienen carácter general, es decir, no se hace distinción respecto al tipo de infracción cometida, sino que se pena la inobservancia de cualquiera de las disposiciones contenidas en la ley.

Así, el incumplimiento del derecho de información no encuentra una sanción específica, de manera que la sanción deberá regularse por la Superintendencia correspondiente, dentro del marco trazado que establece las siguientes sanciones:

- Multas de hasta mil quinientos salarios mínimos⁹¹, que traducidos a pesos chilenos corresponden a alrededor de \$211.272.000 pesos chilenos.

- Suspensión de las actividades del banco de datos hasta por un término de seis meses.

- Clausura temporal o definitiva de las operaciones del banco de datos en los casos más graves.

Para graduar las sanciones las Superintendencias deberán atender a la dimensión del daño o peligro para los intereses tutelados en la ley, al beneficio económico obtenido por el infractor, a la reincidencia, a la resistencia al ejercicio de las facultades del

⁹¹ El Salario Mínimo Mensual Legal Vigente se fija anualmente por la Comisión Permanente de Concertación de Políticas Salariales y Laborales y durante el año 2009 corresponder a 515.000 pesos colombianos que traducido a pesos chilenos es equivalente a alrededor de \$140.848, según conversión de monedas a marzo de 2010.

órgano de control, a la renuencia o desacato a cumplir y al reconocimiento de la infracción del órgano incumplidor.

3.1.4. Los derechos del titular a controlar sus datos personales y a ser informado en la Constitución mexicana y en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

La Constitución de los Estados Unidos Mexicanos de 1917 ha sido objeto de numerosas modificaciones para hacerla compatible con el ejercicio de los derechos de protección a los datos personales. El avance ha sido lento y progresivo, abriéndose paso a este camino a través de una primera modificación al artículo 6 que en sus fracciones II y III estableció que los datos personales y la información relativa a la vida privada serán protegidos, así como el derecho a acceder y corregir los datos personales que obren en archivos públicos. El legislador quiso establecer límites al ejercicio del derecho de acceso a la información pública en los tres órdenes de gobierno: federal, estatal y municipal pero no creó un derecho fundamental independiente de amplios alcances.

Así, se establece en el artículo 6:

“Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos”.

Más tarde, mediante Decreto Supremo publicado en el Diario Oficial de la Federación el 1 de junio de 2009, se adicionó un segundo inciso al artículo 16 de las garantías individuales, que consagra un derecho independiente a la protección de datos personales y a la facultad de controlar la información que le concierne al propio individuo, constituyéndose en un derecho de amplios alcances ya que también incluiría los bancos de datos en manos de privados.

Señala el inciso 2 del nuevo artículo 16:

“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.

Con esta disposición estaría clara la facultad del titular de controlar sus datos en manos de órganos públicos y privados. Sin embargo, se conserva un tema pendiente y que dice relación con la existencia de una ley general que desarrolle los derechos ya consagrados a nivel constitucional. En México, desde el año 2000, se promovieron diversos proyectos legislativos en torno a la protección de datos personales en posesión de los particulares en el Congreso de la Unión, sin que ninguno de ellos fructificara dado que, en ese entonces, se carecía de una disposición constitucional que les diera sustento.

Fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el primer instrumento normativo que recogió un capítulo de protección de datos personales, únicamente aplicable a los sujetos obligados en el ámbito público federal. La finalidad de esta ley radica en proveer lo necesario para garantizar el

acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal, siendo sujetos obligados en particular:

- El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;
- El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;
- El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;
- Los órganos constitucionales autónomos;
- Los tribunales administrativos federales, y
- Cualquier otro órgano federal.

Quedó pendiente entonces la aprobación de una ley general que, además del sector público alcanzará el sector privado, en todo el territorio nacional, observando los principios de protección de datos personales y garantizando los derechos de acceso, rectificación y cancelación. Analizaremos, por el momento, como se desarrolla el derecho del titular de los datos a controlar sus datos personales y a ser informado en la única ley mexicana que desarrolla la protección de los datos personales en su capítulo IV.

1. Derecho a ser informado al recabar datos personales del individuo.

Señala el artículo 20 apartado III que los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, un documento en el que se establezcan:

“Los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61.”

Este derecho a ser informado se materializa entonces en la puesta a disposición de un soporte material en el que conste la finalidad que trasciende al tratamiento de datos personales. La ley no señala explícitamente como se efectuará la puesta a disposición, concluyéndose que la modalidad de entrega del documento se determinará por el Instituto⁹² o la instancia equivalente a que se refiere el artículo 61⁹³.

2. Derecho a ser informado manifestado como derecho de acceso.

El artículo 24 de la ley consagra la facultad del titular de la información a acceder a sus datos personales. Así se señala, que sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales.

La unidad de enlace o su equivalente deberá entregarle al titular, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos datos.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío, de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán atendiendo a los márgenes prescritos por el artículo 27.

Los costos por obtener la información no podrán ser superiores a la suma de:

⁹² Instituto Federal de Acceso a la Información establecido en el Artículo 33 la Ley Federal de Transparencia y Acceso a la Información Pública.

⁹³ El artículo 61 se refiere a cómo se realiza la determinación de los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios y plazos establecidos.

- I. El costo de los materiales utilizados en la reproducción de la información, y
- II. El costo de envío.

3. Derecho a ser informado manifestado como derecho de consulta al listado de los sistemas de datos personales.

El artículo 23 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental dispone que los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlos de conocimiento del Instituto o de las instancias equivalente previstas en el artículo 61, quienes tienen el deber de mantener un listado actualizado de los sistemas de datos personales.

Este precepto consagraría el principio de publicidad de los ficheros de datos personales en manos de entidades públicas. Sin embargo, nuevamente, la ley no especifica expresamente si existe un derecho del titular de los datos a consultar el listado. Es forzoso concluir, en armonía al espíritu de la ley y, en general, de los sistemas de protección de datos personales, que el titular efectivamente tiene derecho a consultar este listado y saber, como mínimo, si existe algún fichero en que consten sus datos personales.

4. Derecho a ser informado manifestado como derecho de modificación.

De acuerdo al artículo 25 de la ley, las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales.

La forma de ejercer este derecho es a través de la entrega de una solicitud de modificación a la unidad de enlace o su equivalente, que señale:

- El sistema de datos personales.
- Las modificaciones por realizarse.

- La documentación que motiva la petición, la que deberá ser aportada.

Una vez realizada la solicitud de modificación, la unidad de enlace o su equivalente deberán entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud:

- a) Una comunicación que haga constar las modificaciones.
- b) O bien, la información, de manera fundada y motivada, de las razones por las cuales no procedieron las modificaciones.

Incumplimiento del deber de información en sus diferentes manifestaciones.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental contempla un recurso de revisión que debe interponerse dentro de los quince días hábiles siguientes a la fecha de la notificación, ante el Instituto o ante la unidad de enlace que haya conocido el asunto. El recurso procederá por las siguientes causales:

- i. Negativa de entregar o corregir datos personales.
- ii. Falta de respuesta en los plazos señalados.

De acuerdo al artículo 63, serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en la ley las siguientes, en relación a los derechos de información en sus distintas manifestaciones:

- Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a la ley.
- Denegar intencionalmente información no clasificada como reservada o no considerada confidencial conforme a la ley.

- Entregar intencionalmente de manera incompleta información requerida en una solicitud de acceso (conducta considerada grave para efectos de su sanción administrativa).
- No proporcionar la información cuya entrega haya sido ordenada por los órganos o el Poder Judicial de la Federación.

Estas responsabilidades o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en la ley, son sancionadas en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, considerándose grave, para efectos de su sanción administrativa, la reincidencia en las conductas previstas.

Las responsabilidades administrativas que se generen por el incumplimiento de las obligaciones son independientes a las responsabilidades de orden civil o penal que procedan.

3.2. LEGISLACIÓN CHILENA.

3.2.1. La protección constitucional chilena frente al tratamiento de datos personales.

Las diferentes legislaciones sobre protección de datos personales arrancan su legitimidad de un texto constitucional determinado que consagre derechos y deberes concordantes con las finalidades trazadas para el nuevo texto legislativo, que nace a la vida del derecho para complementar las materias que no pudieron ser desarrolladas cabalmente en la Carta Fundamental, sea por su extensión, por su temporalidad o por otros motivos.

El problema de fondo que reside en la protección de datos personales se centra en el conflicto que podría suscitar la consagración de derechos de esta naturaleza a nivel constitucional, o bien, la posibilidad real de expandir el contenido de los aquellos ya consagrados con la finalidad de hacer frente a los nuevos fenómenos tecnológicos.

Los derechos consagrados en nuestra Constitución de 1980 y que pueden invocarse en relación a la protección de datos personales, son los siguientes:

- Artículo 19 N°4:

La Constitución asegura a todas las personas:

“El respeto y protección a la vida privada y pública y a la honra de la persona y su familia.”

En cuanto a la consagración de la protección a la esfera íntima de las personas originalmente se propuso el respeto a la “intimidad”, sin embargo, existieron opiniones divergentes en introducir dicho concepto en razón, según se adujo, que la garantía de protección más adecuada y completa era la noción de “privacidad”⁹⁴. En opinión del comisionado Guzmán Errázuriz envolvía el ámbito de una zona de la vida de la persona que debe quedar precisamente excluida de la noticia o de la invasión externa. Agrega dicho comisionado que:

“... La intimidad es todavía una zona más profunda y sensible que la privacidad, Es algo todavía más sutil y por lo tanto de menor alcance en su extensión...”⁹⁵.

⁹⁴ ANGUITA Ramírez, Pedro, La Protección de Datos Personales y el Derecho a la Vida Privada, Régimen Jurídico, Jurisprudencia y Derecho Comparado, Santiago, Editorial Jurídica de Chile, 2007, Pág. 126.

⁹⁵ Intervención del Comisionado Jaime Guzmán Errázuriz, Actas Oficiales Comisión Constituyente, Volumen N° 3, Garantías Constitucionales, sesión 129°, celebrada el 12 de junio de 1975, Pág. 2.

Sobre la conveniencia de conceptualizar esta protección con la expresión a la “vida privada” en vez del concepto “privacidad” aduce que:

“... La primera expresión está más desarrollada en el lenguaje común, pues existiría una especie de reconocimiento en la colectividad de que lo que se respeta es la vida privada. No es la vida hacia el exterior; es la vida interna, dentro del hogar; y la privacidad es un término menos usado, menos conocido. En cambio, la forma “vida privada” constituye una referencia permanente...⁹⁶”.

Así se ha plasmado en nuestra Carta Fundamental el respeto y protección a la vida privada, dotándola de un contenido íntegro, con el objetivo de satisfacer la necesidad de un ámbito propio y reservado, necesario para mantener una determinada calidad de vida mínima y cautelando el desarrollo armónico de la personalidad, sin injerencias externas.

La expresión vida privada, no es susceptible de una definición exhaustiva y para concretar su ámbito de protección muchas veces se recurrió a su contraposición con la vida pública, de modo que no se produciría injerencia en la vida privada, en el caso de que se fuera parte de un proceso judicial, pues este aspecto pertenecería al ámbito de la vida pública.

Con el desarrollo del concepto se ha podido establecer que comportamientos realizados de forma pública o en espacios públicos, también pueden pertenecer al ámbito de la vida privada, de manera que no es factible restringir la noción de vida privada, en nuestra Constitución, a un ámbito íntimo o doméstico, pues espacio público y vida privada no son conceptos excluyentes, disponiendo nuestra Carta Fundamental que se respeta y protege tanto la vida privada como la pública.

⁹⁶ Intervención del Comisionado Jaime Guzmán Errázuriz, Actas Oficiales Comisión Constituyente, Volumen N° 3, Garantías Constitucionales, sesión 129°, celebrada el 12 de junio de 1975, Pág. 14.

Lo relevante aquí es subrayar que la interpretación deber ser extensiva, de manera que no se garantiza sólo una esfera interna de la personalidad, como el nombre, la identidad, la vida sexual, la integridad física y moral, la estabilidad mental, etc. Sino que también se protege el derecho a la identidad, el desarrollo personal y el derecho a establecer relaciones con otras personas, sean del tipo que sean, y con el mundo exterior, excluyendo del ámbito de protección a aquellas actuaciones que puedan perjudicar o perturbar la vida de terceras personas ajenas a estas relaciones.

De aquí que se pueda sostener que en relación al respeto y protección de la vida privada se pueden distinguir dos tipos de protección, es decir, una de índole positiva y otra de tipo negativo. En el primer caso, que es el paradigma clásico, la protección de la vida privada se expresa como un derecho destinado a cautelar a las personas frente a intromisiones ilegítimas en su esfera íntima. En el segundo, la protección a la vida privada se extiende más allá y se concreta en la posibilidad de conocer, acceder y controlar las informaciones concernientes al propio individuo⁹⁷ y que encaja precisamente con aquella facultad que postula el nuevo concepto de autodeterminación informativa.

Este aspecto positivo de la vida privada permitiría asentar la idea de que el individuo tiene efectivamente la facultad de controlar la información que le concierne, decidiendo cómo y en qué medida consiente la comunicación a terceros de su información personal, ejercitando su derecho a la vida privada informativa.

⁹⁷ Proyecto de Ley, Mensaje N° 687 – 356 de S.E. la Presidenta de la República con el que inicia el Proyecto de Ley que introduce modificaciones a la Ley N° 19.628 y a la Ley 20.285, Santiago, Chile, 26 de agosto de 2008, Pág. 2.

Por lo tanto, cuando la Constitución chilena consagra la garantía constitucional de la protección a la vida privada de las personas, se están incluyendo las facultades de exclusión y control⁹⁸ que se emplean en el derecho continental.

Esta consideración es importante pues confirma que, sin perjuicio, que nuestra Constitución no consagre expresamente el derecho de controlar la información personal, a través de la ley puede desarrollarse acabadamente la existencia de este derecho y su contenido asociado, que será más extenso a la vida privada para hacerlo compatible con las nuevas necesidades que se presentan en la sociedad de la información.

- Artículo 19 N°12:

La Constitución garantiza a todas las personas:

“La libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley, la que deberá ser de quórum calificado”.

Este precepto consagra el derecho de información, que se ha configurado como la facultad de participación ciudadana en una sociedad democrática y que permite a los individuos solicitar información oportuna, adecuada y veraz. Mediante la utilización racional de la información se posibilita la toma de decisiones informadas.

El antagonismo de este derecho, que pareciera vislumbrarse en una primera aproximación, es sólo aparente, ya que está dispuesto al servicio de los individuos

⁹⁸ GONZÁLEZ Hoch, Francisco, Modelos comparados de protección, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobre protección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, Pág. 156.

integrantes de la sociedad. Es incompatible con un Estado democrático desvirtuarlo al nivel de amparar a las empresas privadas que recolectan información personal de los individuos, o al mismo Estado en el ejercicio de esta labor, efectuándose un ejercicio incompatible con los derechos de los individuos.

- Artículo 19 N°21:

La Constitución 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.”

Algunos autores se han aventurado a señalar que la libre iniciativa privada para desarrollar cualquiera actividad económica está fuertemente plasmada en la Ley de Protección a la Vida Privada, ya que es indudable que ésta contiene, aunque no lo sea en su totalidad, el marco legal que regula la actividad económica – esto es lucrativa – de tratamiento de datos⁹⁹.

Este derecho junto al estatuto social de la propiedad, llevaría a afirmar que la persona que realiza operaciones de tratamiento de datos y construye un registro o banco de datos de los mismos, tiene un derecho de propiedad sobre la base de datos que goza de reconocimiento y protección constitucional, reconociéndose al titular del registro el ejercicio exclusivo de las facultades de dominio correspondientes.

Una afirmación de esta naturaleza desarticula todo el sistema de protección de datos personales, las garantías que se disponen para el titular de los datos y las obligaciones que debe sobrellevar el responsable del registro.

⁹⁹ BERTELSEN Repetto, Raúl, Datos personales: Propiedad privada, libre iniciativa particular y respeto a la vida privada, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobre protección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, Pág. 118.

Afirmar que la libre iniciativa privada para desarrollar cualquier actividad económica es un derecho de carácter preferente ante el derecho a la vida privada, desvirtúa la real dimensión de este derecho que está consagrado al servicio de los individuos y no de la manera inversa, de forma que su ejercicio debe ser compatible con las disposiciones consagradas en beneficio de las personas que componen la sociedad.

No debemos olvidar que la circunstancia de que un ente privado o el Estado efectúen tratamiento de datos personales sobre información concerniente a determinada persona, no implica en modo alguno, que esta información se transfiera a su titularidad. El titular del banco de datos podrá tener derechos de dominio sobre el tipo de organización y su estructuración pero no sobre el contenido intrínseco constituido por la información, la que siempre pertenecerá al propio titular de los datos.

3.2.2. La Ley N° 19.628 sobre Protección a la Vida Privada. El bien jurídico tutelado, sus principios formadores y los derechos del titular de los datos.

Con fecha 5 de enero de 1993, a través de la moción presentada por el entonces senador Eugenio Cantuarias Larrondo, comenzó la discusión de la que pretendía ser la nueva “Ley sobre Protección Civil de la Vida Privada”, aspirando abarcar numerosos tópicos sobre este derecho y otros estrechamente vinculados¹⁰⁰. Sin embargo, contrariamente a lo que su título sugería, el proyecto original fue reducido manifiestamente, aprobándose sólo respecto a aquella parte de la vida privada que se concreta en la protección de los datos personales o datos digitales.

La ley de datos personales tuvo en consideración modelos legales comparados de España, Francia y Gran Bretaña. Respecto a la experiencia desarrollada en Chile, sólo

¹⁰⁰ El Proyecto de Ley original comprendía los derechos a la propia imagen, a la intimidad personal y familiar, al anonimato y reserva, a una vida tranquila, sin hostigamientos ni perturbaciones; y, a la inviolabilidad del hogar y de toda forma de comunicaciones privadas.

se pudo recurrir al Boletín de la Cámara de Comercio de Santiago que data de 1928 y a los informes de Dicom, como empresa filial de Equifax. Precisamente, por esta falta de experiencia el legislador se vio forzado a recurrir a legislaciones de otros países para confeccionar el proyecto, remitiéndose constantemente a derechos foráneos.

De aquí que se discutiera, incluso, la factibilidad de establecer la autodeterminación informativa de las personas respecto de sus datos personales de una manera similar a aquella consagrada en Alemania. Sin embargo, se desechó esta posibilidad, estimándose que aún no era un tema pacífico, ya que las voces disidentes advertían una posible patrimonialización de los derechos del individuo frente a sus datos personales.

Especialmente se tomó como ejemplo la ley española, tanto 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 principios que rigen la ley española (consentimiento, datos especialmente protegidos, calidad de los datos, medidas de seguridad, deber de secreto y cesión de los datos)¹⁰¹ .

Finalmente, en agosto de 1999 se promulgó la Ley N° 19.628 de Protección a la Vida Privada, regulando de una manera muy específica el tratamiento de los datos de carácter personal en registros o bancos de datos. Pese al esfuerzo, la concreción legislativa de la tutela a la vida privada, reflejó que el problema de la protección legal de datos personales frente al tratamiento computacional de los mismos, es un tema que en Chile constituye una realidad desconocida y poco estudiada.

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

¹⁰¹ GONZÁLEZ Hoch, Francisco, Modelos comparados de protección, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobre protección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, Pág. 176.

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.

Procederemos a estudiar entonces cuál es el marco regulatorio del tratamiento de datos personales para los titulares y los obligados:

1. Sobre los titulares.

Los titulares del derecho reconocido en la Ley de Protección de la Vida Privada son las personas naturales, incluso los menores de edad, tal como señala el artículo 2 letra ñ) de la ley.

En cuanto a las personas jurídicas esta ley no les reconoce ninguna titularidad. Este ha sido un punto polémico pues en otras legislaciones se les reconoce siempre protección a las personas jurídicas, mientras en otros casos, sólo de forma matizada respecto de derechos que por su propia naturaleza pueden disfrutar.

Las personas jurídicas difícilmente podrán alegar derecho a la vida, derecho a la vida familiar, vida sexual, vida íntima o integridad corporal, pero por el contrario, podrían alegar efectivamente defensa de su derecho contra escuchas telefónicas, respeto al domicilio o a la correspondencia, que ciertamente son datos personales.

2. Sobre los obligados.

Respecto a los sujetos obligados por la Ley de Protección a la Vida Privada debemos comenzar estableciendo que el primer obligado es el Estado y todos sus organismos públicos, las autoridades, órganos del Estado, organismos, descritos y regulados por la Constitución Política de la República, los comprendidos en el inciso segundo del artículo 1° de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de Administración del Estado.

Por lo tanto, nuestra ley protege a las personas naturales de las injerencias de los poderes públicos. Hace extensible también, esta protección, sin distinciones, frente a las personas jurídicas privadas e incluso a las personas naturales.

Así, en su primer artículo, la ley dispone:

“El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley”.

3. Sobre las obligaciones del titular del fichero.

Ya hemos establecido quiénes son los obligados a respetar las disposiciones de la Ley de Protección a la Vida Privada. Es importante, establecer cuáles son las obligaciones a las que están sujetos los organismos públicos, las personas jurídicas privadas y los particulares que traten datos de carácter personal en registros o bancos de datos.

Como señalamos, el derecho a la protección de datos personales forma parte del derecho a la vida privada que constituye esencialmente un derecho de defensa, sin embargo, por las características que presenta el tratamiento de datos personales, fue necesario otorgar ciertas facultades que materializaran la protección de los datos personales.

Estas facultades de disposición y control de los propios datos se concretan como un derecho a que el titular del banco de datos, realice determinadas acciones tendientes a la protección de los datos de carácter personal.

Las obligaciones contempladas son las siguientes:

- a) Obligación de informar:

Los responsables de los ficheros tienen la obligación de informar al titular de los datos de aquellos ficheros en que constan sus datos personales.

Esta obligación de información se materializa en los siguientes puntos a informar:

a. Como señala el artículo 3 de la Ley N° 19.628, en el caso de recolecciones de datos personales realizadas a través de encuestas, estudios de mercado o sondeo de opinión pública u otros instrumentos semejantes, se deberá informar a las personas sobre el carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

b. Como señala el artículo 4 de la Ley N° 19.628, una de las hipótesis en las que procederá el tratamiento de datos personales, consiste en aquella en que el titular consienta en el tratamiento.

Para que el titular de los datos esté en posición de consentir, debe ser debidamente informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

c. Como señala el artículo 12 de la Ley N° 19.628, el titular de los datos tiene derecho a exigir a quién sea responsable del fichero, que se le informe sobre los datos relativos a sus persona. Extendiéndose esta información a señalar la procedencia de los datos, su destinatario, el propósito del almacenamiento y la individualización de las personas y organismos a los cuales se han transmitido regularmente datos.

b) Obligación de confidencialidad y secreto:

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

Así dispone el artículo 7 de la Ley N° 19.628 al establecer un principio de reserva y fijar medidas que protegen los datos de carácter personal contra riesgos de acceso inadecuado. Por lo tanto, lo que se persigue es mantener la confidencialidad e integridad de los datos personales frente a actos exteriores que puedan poner en peligro y, consecuentemente, perjudicar los intereses y derechos individuales.

c) Obligación de seguridad en el tratamiento:

Este deber estipula que deben establecerse las medidas necesarias para la protección de los datos personales con el fin de evitar su destrucción accidental o no autorizada, su pérdida, acceso, modificación y difusión de los mismos de forma irregular.

d) Obligación de mantener registrados datos de calidad:

La Ley N° 19.628 acoge esta obligación cuando establece la obligación de garantizar la veracidad y vigencia de los datos, enmarcados en un tratamiento lícito. De esta forma, se establecen los siguientes deberes:

a. Modificación: cuando los datos personales objeto de tratamiento sean erróneos, equívocos o incompletos.

b. Eliminación: cuando los datos objetos de tratamiento hayan devenido en caducos o su tratamiento carezca de fundamento legal.

c. Bloqueo: cuando sobre los datos objeto de tratamiento no pueda establecerse su vigencia o ésta sea dudosa y respecto de los cuales no corresponda cancelación.

Este deber establecido en el artículo 6 de la Ley de Protección a la Vida Privada, va aún más allá, cuando establece que en el caso que los datos personales 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 en el caso de no ser posible la determinación de las personas a quienes se les hayan

comunicado, publicará un aviso que pueda ser de general conocimiento para quienes usen la información, tal como dispone el artículo 12 de la ley.

Reforzando estos deberes, se reconocen determinados principios establecidos en torno a la calidad de los datos:

- Principio de Lealtad: conforme a este principio los datos deben ser obtenidos y tratados de forma leal y lícita. Este principio hace referencia, principalmente, a las circunstancias en que los datos han sido obtenidos y ofrece la posibilidad de que los titulares de los datos, al saber qué datos suyos han sido recogidos, puedan ejercer determinados derechos como el de acceso y rectificación.

- Principio de Finalidad: en todo proceso de tratamiento de datos personales, los datos deben ser recogidos para fines determinados y legítimos, y no deben ser utilizados de manera incompatible con tales fines trazados. Este principio debe respetarse con antelación al inicio del tratamiento de datos personales, pues sólo así se podrá comprobar si los datos están siendo utilizados de acuerdo a la finalidad para la que fueron recogidos.

- Principio de Pertinencia: los datos deben ser adecuados, pertinentes y no excesivos respecto a los fines para los que fueron recogidos, en un aspecto cualitativo y cuantitativo. Este principio se vincula con el principio de finalidad, pues sólo estableciendo los datos en relación con los fines para los que se recogieron podremos comprobar si éstos cumplen con este principio de pertinencia, es decir, si son datos pertinentes y adecuados que no inducen a error sobre la finalidad del tratamiento y si se han recogido sólo aquellos datos necesarios para la finalidad que se persigue con el tratamiento.

- Principio de Exactitud: los datos recogidos y almacenados deben ser exactos y actuales, es decir, deben irse poniendo al día, evitando los perjuicios que podrían provocarse al titular de los datos por la existencia de errores o datos no fiables.

- Principio de Conservación: los datos deben ser conservados de tal forma y durante un período de tiempo tal que sólo permita identificar a los titulares de los mismos durante el plazo que sea necesario para conseguir los fines para los que fueron recogidos.

4. Control del tratamiento de datos personales.

Cabe ahora referirse al sistema de control y garantías que establece la Ley N° 19.628 y que se preceptúa entre los artículos 20 a 23.

a) Órgano fiscalizador.

Señala la Ley N° 19.628 que el Servicio de Registro Civil e Identificación llevará un catastro de los bancos de datos personales a cargo de organismos públicos. Es decir, el registro está sólo contemplado para el caso de tratamiento de datos personales por parte de autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política de la República, 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 al tratamiento de datos realizado por organismos privados y particulares no existe ninguna modalidad de registro, de manera que los titulares de datos personales no tienen un organismo específico o autoridad a la que acudir para hacer valer sus derechos y que impulse el desarrollo del principio de publicidad.

Respecto al catastro a cargo del Servicio de Registro Civil e Identificación se contempla que éste tendrá un carácter público y en él constarán los siguientes puntos respecto a los datos personales tratados por organismos públicos:

- El fundamento jurídico de la existencia del banco de datos.
- La finalidad del banco de datos.
- El tipo de datos almacenados.

- La descripción del universo de personas que comprende.

Puede vislumbrarse que las soluciones otorgadas en la ley son insuficientes. El sistema no tiene un alcance generalizado para ejercer funciones fiscalizadoras a todos los bancos de datos, independientemente de la naturaleza del titular del fichero, más aún el control de las actividades centradas en el tratamiento de datos personales se le entrega a un organismo que no cumple los requisitos de independencia y autonomía propias y necesarias para la efectividad de la autoridad de control.

- b) Responsabilidad por infracciones.

Cuando nos encontremos frente a un caso de tratamiento indebido de datos, el organismo público, la persona jurídica de derecho privado o el particular responsable del banco de datos personales deberán indemnizar por el daño causado.

Respecto al alcance del daño, se indemnizará tanto el daño patrimonial como el moral. Sin perjuicio de las indemnizaciones correspondientes, el responsable del fichero deberá proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, a aquello que ha ordenado el tribunal correspondiente.

- c) Acción de reclamación y acción indemnizatoria.

La reclamación destinada a establecer la infracción se refiere a los casos contemplados en el artículo 16 y 19 de la Ley N° 19.628.

Cuando el responsable del registro no se pronuncie sobre la solicitud del titular de los datos en cuanto a requerir información, modificación, cancelación o bloqueo de los datos personales registrados, dentro del plazo de 2 días hábiles, o la denegare por causa distinta de la seguridad de la Nación o el interés nacional, surge el derecho para el titular de recurrir ante el Juez de Letras en lo Civil del domicilio del responsable, solicitando amparo a los derechos consagrados.

La acción indemnizatoria puede ser interpuesta conjuntamente cuando se interponga acción de reclamación destinada a establecer la infracción.

La acción civil indemnizatoria 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 afecto (Artículo 23).

3.2.3. Desarrollo del derecho de información del titular del los datos personales y la efectividad de las tutelas ofrecidas en la ley.

Tal como adelantamos en el punto anterior, la Ley N° 19.628 establece en diversos artículos el derecho a ser informado que detenta el afectado frente al tratamiento de datos personales. Analizaremos ahora en profundidad como se desarrollan estas potestades a través de los preceptos.

1. Derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública.

El artículo 3 dispone:

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

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

Este artículo está dispuesto para regular la actividad de los órganos públicos, personas jurídicas privadas o particulares que realicen actividades de fines

estadísticos indefinidos, ya sea a través de encuestas, sondeos de mercado u opinión pública, los que se materializarán mediante la realización de un serie de preguntas normalizadas y dirigidas a una muestra que se considerará representativa de determinado segmento de la población o instituciones.

El objetivo general de estas herramientas es conocer estados de opinión o hechos determinados que permitan trazar una visión representativa de un público de mayores dimensiones, contemplándose, simultáneamente, uno o más objetivos específicos, que podrán fluctuar, por ejemplo, entre los siguientes:

- Calcular las relaciones entre variables demográficas, económicas y sociales.
- Evaluar las estadísticas, sus errores, omisiones e inexactitudes.
- Establecer patrones de las variables demográficas y sus factores asociados como fecundidad y migraciones determinantes.
- Otorgar información suplementaria en relación a la otorgada por los censos.
- Apreciar periódicamente los resultados de un programa en ejecución.
- Probar la eficiencia de un método antes de aplicarlo al total de las personas originalmente contempladas.
- Saber la opinión del público acerca de un determinado tema.

El derecho de información se aplicará en estos casos para aquel individuo que conteste las preguntas realizadas por el encuestador y se extenderá a los siguientes puntos:

- i. Sobre el carácter obligatorio o facultativo de las respuestas.

Cuando se recolecta información a través de alguna de estas técnicas, suele utilizarse como métodos la entrevista, la encuesta telefónica o el correo. Esto implica que para recoger la información, el individuo está consciente de aquello que está ocurriendo, es decir, es él quién comunica directamente el elemento informacional, de manera que se encuentra en posición de discernir las consecuencias que se derivan de esta actividad. En este sentido, las personas saben que ante una encuesta, sondeo de

mercado u opinión pública la emisión de respuestas es facultativa y no obligatoria. Por esta razón, el derecho a ser informado, que se le otorga al encuestado se manifiesta en un grado atenuado.

ii. Sobre el propósito para el cual se está solicitando la información.

Aquel individuo que ha decidido responder las interrogantes realizadas por el encuestador debe ser informado respecto al objetivo que trasciende a la encuesta, sondeo de mercado u opinión pública expresando su voluntad o intención, el que dependerá del tipo de formato escogido pero que a grandes rasgos redundará en que a través de las respuestas obtenidas de un segmento determinado de individuos se pueda obtener un parámetro de las necesidades o preferencias sobre algo o alguien y en base a estos resultados se tomen decisiones informadas. Delineándose este objetivo general deben definirse los objetivos específicos que se han contemplado y que podrán ser de variada naturaleza.

2. Derecho a ser informado para autorizar el tratamiento de datos personales.

El artículo 4 dispone en su inciso 1 y 2:

“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”.

Este artículo regula los casos en los que se permite efectuar operaciones o procedimientos técnicos 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. Será procedente realizar alguna de estas actividades únicamente en los siguientes casos:

a) Cuando la Ley de Protección a la Vida Privada u otras disposiciones legales lo autoricen.

b) Cuando el titular consienta expresamente en ello a través de una autorización que deberá constar por escrito y que está sujeta a revocación, de acuerdo a lo dispuesto en los incisos 3 y 4.

En el caso que el titular de los datos autorice, tiene derecho a ser informado respecto a:

i. El propósito del almacenamiento de sus datos personales, debiendo especificarse el objetivo, intención o fin que reside en la recolección de datos y su tratamiento asociado.

ii. La posible comunicación al público de sus datos personales, de manera que el titular del banco de datos deberá comunicar que podría realizarse una eventual transmisión de su información personal.

Hasta aquí podemos identificar algunos inconvenientes de la Ley de Protección a la Vida Privada en cuanto a una evidente debilidad del derecho a ser informado:

1. En el caso que la misma ley u otras disposiciones legales autoricen el tratamiento de datos, el derecho a ser informado que debería contemplarse para el titular de los datos personales simplemente no se otorga. Se entiende que sólo se detenta este derecho cuando se requiere el consentimiento a través de la autorización del afectado.

2. La extensión que se otorga al derecho a ser informado es en extremo superficial ya que se extiende sólo a señalar el propósito del almacenamiento de datos y su posible comunicación al público, de manera que el afectado queda en indefensión

frente a una transmisión masiva de sus datos, estando imposibilitado de conocer a quienes se ha transmitido su información personal.

El problema toma importantes dimensiones cuando se advierte que si bien pareciera que la intención de legislador fue establecer casos muy limitados en los que se permite efectuar tratamientos de datos personales, esta pretensión de acotar o reducir estos casos se esfuma rápidamente al analizar los próximos incisos.

Los incisos 5 y 6 agregan:

“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”.

De acuerdo a esta amplísima excepción, que inevitablemente se constituirá como la regla general, no se otorgará al afectado el derecho a consentir y a autorizar y, consecuentemente, a ser informado cuando los datos personales procedan de “fuentes accesibles al público”, que en la letra i) del artículo 2 se definen amplia y vagamente 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 disposición es que los datos personales se estimarán por regla general como legalmente públicos y cualquiera podrá procesarlos y comercializarlos porque el acceso a ellos está legitimado por ley sin restricciones.

La primera interrogante a dilucidar versa sobre cuáles son los registros que pueden ser considerados como “de datos personales públicos o privados de acceso no restringido o registrado a los solicitantes”, sin embargo, la ley no efectúa una categorización, de manera que la determinación tendrá que ser realizada por los órganos jurisdiccionales pero para casos concretos, lo que en términos prácticos no solucionará el problema para la generalidad de los casos que no llegan a tribunales.

En Chile se contempla sólo en casos muy específicos determinadas fuentes de información de acceso restringido como el secreto estadístico, el secreto tributario, el secreto bancario o el secreto de filiación política, concluyéndose entonces que todas las fuentes de datos serán, en principio y por regla general, legalmente de acceso público, no restringido o reservado a los solicitantes¹⁰², salvo que una ley especial, una norma, una resolución administrativa o una cláusula contractual establezcan expresamente lo contrario.

Tenemos entonces que atendidas las excepciones, la necesidad de consentimiento informado es sólo una mera declaración de principios, que se torna incluso más extensa cuando la disposición establece específicamente cuáles serán los casos de fuentes accesibles al público en los que se puede prescindir de la autorización del afectado y del deber de información correlativo:

¹⁰² JIJENA Leiva, Renato, La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobreprotección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, Pág. 99.

- i. Cuando sean datos de carácter económico, financiero, bancario o comercial.

Cuando la ley se refiere a estos datos no existe claridad en relación a qué tipo de información se está pronunciando, es decir, si se considera de fuente accesible al público la información negativa, la positiva o ambas.

La información negativa se referirá a todos los datos vinculados con protestos de letras, cheques y pagarés, y cuotas morosas impagas, que tienen las personas naturales y jurídicas con el sistema financiero comercial en su conjunto¹⁰³, justificándose por sí sola, en el sentido que su promoción tiene por objetivo prevenir al mercado sobre aquellos individuos que tienen conductas comerciales desordenadas¹⁰⁴. Mientras, la información positiva, se refiere a un concepto más amplio relacionado con el comportamiento de pago que ha tenido históricamente una persona, la deuda que se encuentra todavía vigente en el mercado y los datos patrimoniales generales de los individuos.

Pese a que la Ley de Protección a la Vida Privada no distingue a qué datos se refiere, de acuerdo a las disposiciones que rigen a la Superintendencia de Bancos e Instituciones Financieras, se prohíbe a instituciones no reguladas por la Superintendencia de Bancos e Instituciones Financieras consultar o adquirir información positiva del endeudamiento de las personas en el sector financiero, por lo que el sector comercio no tendría acceso a ella. Además, esta hipótesis toma más fuerza cuando se observa el título de III de la ley que se refiere a la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o

¹⁰³ ORTIZ, Claudio, La protección de datos personales y la información comercial, en obra colectiva Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?, Santiago, Serie Políticas Públicas, 2009, Pág. 25.

¹⁰⁴ Aún así, el artículo 18 de la Ley de Protección a la Vida Privada limita la comunicación de los datos negativos cuando transcurran siete años desde que la respectiva obligación se hizo exigible o cuando hayan transcurridos tres años desde el pago o la extinción por otro modo legal.

comercial, individualizando en el artículo 17 cuáles obligaciones son comunicables, marginándose de esta lista a la información positiva.

Sin embargo, el hecho de que este tema no esté regulado tajantemente en la Ley de Protección a la Vida Privada es una falencia que puede prestarse para numerosos inconvenientes respecto al eventual acceso de organismos, personas jurídicas privadas o particulares que no estén regulados por la Superintendencia de Bancos e Instituciones Financieras, a información positiva de los individuos.

ii. Cuando los datos 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.

El uso de la expresión “tales como” demuestra que esta enumeración es sólo ejemplar y avala la existencia de otros tipos de datos a incluir en esta excepción, siendo una cuestión de hecho definir si cierto dato personal es o no de aquellos contenidos en listados relativos a una categoría de personas que pueden ser tratados prescindiendo del consentimiento informado del titular de la información.

iii. Datos que sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Como ya estudiamos, una de las formas de gestión empresarial más valoradas por las empresas consiste en la actividad de marketing directo, que a través del estudio de bancos de datos, recopila y cruza información, creando perfiles de comportamiento de los individuos que le permiten estratificar y focalizar el segmento hacia el cual apuntará determinada campaña comercial o venta de productos.

Sin embargo, aquello altamente lucrativo para una empresa puede ser profundamente contradictorio con los derechos de las personas que son titulares de los datos personales, pues la existencia o inexistencia de esta relación empresa – cliente, le compete directamente al consumidor, quien podría querer mantenerse al margen de

esta actividad, optando por resguardar su privacidad y no ser abordado con agresivas campañas comerciales, e-mails promocionales, llamados telefónicos, etc.

Este precepto, aprueba y legitima con mínimas limitaciones el marketing directo, primando, incluso, por especialidad frente a la facultad del artículo 3 inciso segundo, que faculta al titular para oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Aún en la hipótesis contraria, será muy difícil para el afectado identificar cuando están siendo utilizados sus datos para marketing directo, estando imposibilitado de ejercer su derecho de oposición.

vi. Otra excepción encubierta que contempla el artículo 4 en su último inciso y que faculta a prescindir del deber de información al afectado se refiere a los casos en que el tratamiento de datos personales sea realizado por personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades que están afiliadas, con fines estadísticos de tarificación u otros de beneficio general de aquéllos.

Análogamente a los casos anteriores, este precepto es de una extensión amplísima, es decir, faculta a las personas jurídicas privadas para realizar tratamiento de datos personales, no sólo de fuentes accesibles al público, sino también de aquellas de acceso restringido. Además, la utilización de esta información se amplía al propio uso de la persona jurídica, de sus asociados y de organismos afiliados, contemplándose como objetivo la recolección, análisis e interpretación de datos para explicar condiciones regulares en fenómenos aleatorios, con la finalidad de determinar las tasas, tipos de primas y precios aplicables a determinados productos, fenómenos y riesgos.

v. Más adelante, la Ley de Protección a la Vida Privada vuelve a realizar otra excepción, estimando que no se requiere del consentimiento del afectado cuando el tratamiento de datos sea realizado por un organismo público, cuando se cumplan las siguientes condiciones:

- El tratamiento de datos se efectúe respecto a materias que son de competencia de este organismo público.
- El tratamiento se realice con sujeción a las normas precedentemente dispuestas.

Así lo señala el artículo 20:

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

3. Derecho a ser informado manifestado como derecho de acceso.

En el título II de la Ley de Protección a la Vida Privada se tratan los derechos de los titulares de los datos. El primer derecho contemplado es el derecho a ser informado manifestado como un derecho de acceso a los datos. En su artículo 12 inciso uno dice así:

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

Este precepto se configura como el derecho de acceso que detenta el titular de los datos personales, que se activa sólo a petición del afectado y al que el titular del fichero está en obligación de cumplir. Podríamos advertir que este tipo de derecho a ser informado se diferencia en un aspecto temporal a aquel contemplado en los artículos 3 y 4, ya analizados, pues aquí el derecho se concede posteriormente a la realización del tratamiento de datos.

Este derecho de acceso se puede ejercer contra organismos públicos y privados, tal como reza el precepto. Sin embargo, cabe aquí hacer una advertencia que refleja otra de las tantas flaquezas de la Ley de Protección a la Vida Privada, respecto al derecho a ser informado, materializado aquí en el derecho de acceso. Como ya adelantamos, esta ley establece la existencia de un registro de los bancos de datos personales, a cargo del registro Civil e Identificación, el problema es que este registro contendrá únicamente los ficheros de los organismos públicos.

La inexistencia de un registro que contenga los bancos de datos cuya titularidad pertenezca a personas jurídicas privadas y particulares, dificultará tanto el derecho de acceso de los particulares a los bancos de datos en que conste su información personal, que se hará derechamente impracticable. En efecto, es factible que los titulares de los datos personales nunca sepan de la existencia del banco de datos o el origen de éstos, de manera que los responsables actuarán en total anonimato y carentes de todo control de la autoridad.

Asimismo señala el precepto que este derecho a ser informado, accediendo a los datos personales que constan en el banco de datos, implica conocer:

- a. Los datos relativos a la persona: imágenes, sonidos, caracteres grafológicos, muestras físicas, etc. que entregan antecedentes que hacen identificable a la persona.
- b. La procedencia de los datos personales contenidos en el fichero: debe definirse cual es el origen de los datos recogidos, si proviene del propio titular, de una transferencia realizada por terceros u otro medio.
- c. El destinatario de los datos personales contenidos en el fichero: individualización del órgano público, persona jurídica privada o persona natural a quien está destinado el tratamiento de datos personales y que hará uso del tratamiento de datos.

d. El propósito del almacenamiento de los datos personales: objetivo general y finalidades específicas que justifican el tratamiento de datos personales.

e. La individualización de las personas y organismos a los cuales los datos son transmitidos regularmente: órganos públicos, personas jurídicas privadas y personas naturales a las que se les comunican los datos personales que están siendo objeto de tratamiento.

4. Derecho a ser informado manifestado como derecho de consulta frente al Servicio de Registro Civil.

La Ley N° 19.628 establece un derecho de consulta frente al Servicio de Registro Civil e Identificación, al que se le otorga la facultad de llevar un registro de los bancos de datos personales, únicamente, a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos:

- a. El fundamento jurídico de la existencia del registro.
- b. La finalidad del tratamiento.
- c. Los tipos de datos almacenados y descripción del universo de personas que comprende.

Se dispone que los detalles de este precepto serán desarrollados por un reglamento.

De acuerdo a esta disposición, existe una obligación para los organismos públicos responsables de bancos de datos de proporcionar los antecedentes señalados al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y cuando se produzca cualquier cambio de los elementos indicados dentro de los quince días desde que se produzca.

Las grandes falencias de este derecho radican en que no abarca a los bancos de datos en manos de privados y que estas facultades deberían haber sido otorgadas a un órgano de control propiamente tal, que tenga la independencia y atribuciones necesarias para garantizar y fiscalizar la protección de los datos personales de las personas.

5. Derecho a ser informado manifestado como derecho de modificación, eliminación y bloqueo.

Además del derecho de acceso que concede el artículo 12, sus incisos 2, 3 y 4 establecen derechos de modificación, eliminación y bloqueo:

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

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

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

Consecuencia del derecho a ser informado, son los derechos de modificación, eliminación y bloqueo que podrán ser ejercidos gratuitamente:

- Derecho de modificación: cuando los datos sean falsos, equivocados, desacertados, carentes de exactitud, defectuosos o imperfectos.

- Derecho de eliminación: cuando los datos no tengan un fundamento legal que justifique su tratamiento, sean obsoletos o anacrónicos o cuando el titular de los datos haya proporcionado los datos voluntariamente o estos se utilicen para comunicaciones comerciales y no desee continuar figurando en el banco de datos, sea de modo definitivo o temporal.

- Derecho de bloqueo: también procede cuando los datos se hayan proporcionado voluntariamente o estos se utilicen para comunicaciones comerciales y no desee continuar figurando en el banco de datos, sea de modo definitivo o temporal.

Puede ocurrir que pese a que se ejerzan estos derechos en el banco de datos original, se haya efectuado una transmisión hacia un tercer órgano público, privado o un particular. En este caso el responsable del banco de datos deberá avisar en un corto plazo la operación efectuada y si no fuera posible determinar estas terceras personas a quienes se haya comunicado los datos, se deberá publicar un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

Es criticable que la norma no haya determinado exactamente el plazo que se tiene para informar la operación de modificación, eliminación o bloqueo, la que quedará, en definitiva, a discreción del responsable del banco de datos. Asimismo, no se especifica las características del aviso que deberá publicarse, los medios aptos, ni tampoco se fija un plazo para realizarlo, quedando entregado, nuevamente, al arbitrio del responsable del fichero.

Limitaciones al derecho a ser informado.

Pese a la existencia del derecho a ser informado contemplado expresamente en el artículo 12, la misma Ley de Protección a la Vida Privada establece que este derecho no es absoluto y tiene limitaciones constituidas por intereses de orden superior.

Así, el artículo 15 señala:

“No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras de organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Tampoco podrá pedirse la modificación, cancelación o bloqueo de los datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva”.

Este precepto estaría contemplado para bancos de datos cuya titularidad pertenezca a organismos públicos y cuando la solicitud de información, modificación, cancelación o bloqueo de datos personales se encuadre en alguna de las siguientes hipótesis:

- Impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido.
- Afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias.
- Afecte la seguridad de la Nación.
- Afecte el interés nacional.
- Los datos hayan sido almacenados por mandato legal, excluyéndose los casos contemplados en la ley respectiva.

Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.

Señala el artículo 16:

“Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se

encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente”.

Esta acción de reclamación ante los tribunales de letras civiles, se contempla únicamente para cautelar el derecho a ser informado del artículo 12¹⁰⁵, que contiene el derecho de acceso y los derechos de modificación, eliminación y bloqueo. En estos casos el titular de los datos personales ha solicitado acceso a sus datos personales y al tomar conocimiento de éstos ha ejercido su derecho a solicitar su modificación, eliminación o bloqueo por procedencia de las causales contempladas en la ley. Frente a esta solicitud el responsable del banco de datos:

- i. No se pronuncia dentro de dos días hábiles respecto a la solicitud de acceso, modificación, eliminación o bloqueo presentada por el titular de los datos.
- ii. Se pronuncia, denegando la solicitud de acceso, modificación, eliminación o bloqueo presentada por el titular de los datos, fundamentándola en causa distinta a la seguridad de la Nación o el interés nacional.

En el caso que el fundamento de la denegación sea efectivamente la seguridad de la Nación o el interés nacional, la reclamación deberá presentarse ante la Corte Suprema.

Si la reclamación se acoge, el responsable del banco de datos deberá, en el plazo establecido por la sentencia, proceder a entregar al titular de los datos la información solicitada o modificar, eliminar o bloquear los datos que corresponda.

Sin perjuicio del ejercicio de la correspondiente acción de reclamación, la infracción al deber de informar al titular de los datos, otorgarle acceso a su información oportunamente y el retardo en el ejercicio de los derechos de modificación, eliminación y bloqueo de los datos personales, en la forma que decrete el tribunal, será castigada

¹⁰⁵ Si el titular de los datos quiere hacer valer los derechos otorgados por el artículo 3 y 4 de la Ley de Protección a la Vida Privada, deberán optar por otro procedimiento, acción o recurso.

con multa de dos a cincuenta unidades tributarias mensuales, es decir, entre \$73.504 y \$1.837.600 pesos¹⁰⁶, como multas generales por infracciones a la Ley N°19.628.

Cabe preguntarse si estas multas son realmente disuasivas, atendido su monto relativamente reducido en comparación al patrimonio de las administradoras de bases de datos. En este sentido, el volumen de los negocios que realizan no establece incentivos suficientemente fuertes para dar cumplimiento estricto a la ley. Puede ocurrir que las administradoras de bases de datos evalúen que resulta más eficiente (en términos de gastos legales, tiempo y multas) pagar las sanciones que adecuarse afectivamente a la ley¹⁰⁷.

Otra de las falencias que presenta la reclamación y las multas infraccionales es que se contemplan tan sólo para el caso de vulneraciones al derecho a ser informado contemplado en el artículo 12 y sus derechos derivados, de acceso, modificación, eliminación y bloqueo de datos.

El problema que se presenta aquí dice relación con cuáles serán los medios otorgados a los individuos que vean vulnerados sus derechos de información contemplados en los artículos 3 y 4 de la ley y cómo podrán esgrimir su defensa, si el derecho de reclamación no se contempla para estos casos. Es relevante recordar, que estos dos casos y en especial el artículo 4, consagran un derecho a ser informado a iniciativa del responsable del banco de datos, que deberá cumplirse en un espacio temporal anterior a aquel contemplado en el artículo 12, pues más allá de sus falencias, se establece como condición para el mismo tratamiento de datos durante la configuración de los respectivos registros. Ante la vulneración de estos preceptos, el afectado no vería otra posibilidad que ejercer sus derechos mediante una acción constitucional de protección.

¹⁰⁶ UTM calculada de acuerdo al mes de marzo de 2010.

¹⁰⁷ GÓNZÁLEZ Hoch, Francisco, Modelos comparados de protección, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobreprotección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, Pág. 178.

El hábeas 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 personales. Sin embargo, la ineptitud de la acción de reclamación dispuesta por la ley de protección de datos personales no radica sólo en su limitada extensión, sino que abarca problemas aún más agudos y que se vinculan a su inoperante desarrollo como una acción específica y autónoma, de objeto definido y tramitación concentrada.

Por sus caracteres definitorios la acción de reclamación debe señalar la infracción cometida y los hechos que la configuran, lo que se contradice bastante con la realidad de los ficheros automatizados que son actividades verdaderamente silenciosas.

Aún así, si el titular de los datos quisiera ir más allá y solicitar la indemnización de los daños que se le han provocado, tal como se le confiere este derecho en la ley, a través del artículo 23 en su primer inciso:

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

El afectado tendría que conducirse de acuerdo al régimen de responsabilidad extracontractual, basado en la culpa del administrador o responsable de la base de datos, lo que implica necesariamente que se pone de cargo de la víctima la carga onerosa de acreditar la culpa o negligencia, lo que es sumamente complicado.

En definitiva, la acción de reclamación y reparación dispuestas, distan mucho de configurarse como recursos efectivos de hábeas data, capaces de poner eficientemente en marcha el aparato judicial para cautelar los derechos de información

de los individuos, junto a sus derechos derivados de acceso, modificación, eliminación y bloqueo y los daños que se deriven de las irregularidades.

CAPÍTULO IV
LAS MODIFICACIONES LEGALES EN CHILE Y SU ADECUACIÓN AL ESTÁNDAR
INTERNACIONAL DE PROTECCIÓN DE DATOS EN MATERIA DE INFORMACIÓN
AL AFECTADO POR EL TRATAMIENTO DE DATOS PERSONALES.

4.1. Proyecto de Ley que introduce modificaciones a la Ley N° 19.628 sobre Protección a la Vida Privada y a la Ley N° 20.285 de Acceso a la Información Pública.

El 26 de agosto de 2008, a través del mensaje 687-356 se dio inicio a un Proyecto de Ley que introduce modificaciones a la Ley N° 19.628 de Protección a la Vida Privada y a la Ley N° 20.285 de Acceso a la Información Pública, sometiéndose a la consideración de la Cámara de Diputados.

El proyecto estima que pese a que la Constitución garantiza en su artículo 19 N° 4 el respeto a la vida privada y pública y a la honra de la persona y su familia en el ámbito de la protección de los datos personales frente a su tratamiento automatizado, sería necesario considerar la relevancia del derecho a la autodeterminación informativa, el que otorgaría al individuo la facultad de control necesaria frente a su información personal, posibilitándolo para construir la dimensión social de su personalidad, autorizando su recolección, conservación, uso y circulación, como asimismo, para conocerla, actualizarla, rectificarla o cancelarla.

En el Proyecto de Ley se señala la necesidad de ampliar y adaptar el concepto de vida privada a las exigencias de un mundo en constante cambio, es decir, se reconoce la necesidad de las sociedades actuales de equilibrar el creciente flujo de información y la garantía de la vida privada de los ciudadanos.

A través de este reconocimiento del derecho a la autodeterminación informativa como una ampliación y adaptación del concepto de vida privada, se establecen una serie de deberes positivos de los poderes públicos e instituciones privadas que preceden al

tratamiento de datos personales, con la finalidad de facultar a las personas para conocer y acceder a las informaciones que les conciernen, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer su transmisión.

Según el proyecto, los fundamentos que justificarían la modificación de la Ley N° 19.628 radican en las insuficiencias que trascienden a la normativa¹⁰⁸. Sin embargo, se reconoce que la creación de la ley en 1998 fue un gran avance en la materia de tratamiento de datos personales ya que hacia esa fecha no existía legislación alguna respecto al tema, pese a los crecientes y progresivos avances tecnológicos. Aún así, queda un largo recorrido para adecuarse al ideal de la normativa internacional de tratamiento de datos personales, en especial al Convenio 108 del Consejo de Europa y a la Directiva 95/46/CE de manera de poder participar en la transferencia de datos personales a terceros países garantizando niveles de protección adecuados.

Entre las principales críticas que recoge el proyecto se encuentran:

- La inexistencia de un registro de responsables privados de bases de datos.
- La inexistencia de un órgano fiscalizador autónomo.
- Haber establecido que la regla general fuera que la información fuera pública y que no requiriese de la autorización de sus titulares para procesarse.
- El no haber prohibido la transferencia internacional de datos personales a terceros países que no posean un adecuado sistema de protección.
- No haber otorgado protección a personas jurídicas.

¹⁰⁸ JERVIS Ortiz, Paula, Modelo de Propuesta Regulatoria al Mercado de Datos Personales en Chile, en Revista Chilena de Derecho Informático N° 8, Centro de Estudios en Derecho Informático, Universidad de Chile, Facultad de Derecho, 2006, Pág. 160. "Nuestro marco regulatorio no asigna en forma clara y eficiente los derechos que en este ámbito se encuentran en disputa: el derecho a tratar los datos personales v/s el derecho a la privacidad informacional; existen varias hipótesis fácticas en las cuales no queda claro en qué persona radica el derecho, como asimismo, han quedado fuera de regulación casos que necesariamente se han debido tomar en cuenta, como lo ha hecho el derecho comparado... El estado actual de la situación muestra que si bien existen reglas legales que aplican al mercado de datos personales en nuestro país, los datos personales que se comercializan, lo son muy generalmente sin autorización por parte de los titulares de datos respectivos, de manera que estos no pueden controlar su información personal (cómo, dónde y para qué se utilizará)..."

- No haber exigido autorización para un cúmulo de actividades relacionadas con el tratamiento de datos personales.

Para reestructurar el marco regulatorio de la Ley de Protección a la Vida Privada, el proyecto propone, en primer lugar, consagrar explícitamente el derecho de las personas a controlar sus datos ya que actualmente sólo se hace referencia al derecho a efectuar tratamiento de datos personales, priorizando el derecho a realizar cualquier actividad económica, contemplado en el artículo 19 N°21 de la Constitución.

En cuanto al derecho a ser informado, que contiene numerosas falencias en la legislación actual, las modificaciones que pretende el proyecto reestructurarían esta facultad a través de las siguientes reformas:

- i. Se amplía el margen de sujetos protegidos por la ley, haciéndose extensible también a las personas jurídicas, de manera que éstas también serán titulares del derecho de acceso, modificación, eliminación y bloqueo cuando corresponda. Se entiende que no existe razón de peso alguna que justifique la marginación de las personas jurídicas del régimen de protección de datos.
- ii. Se fortalecen los derechos de información, ampliándose el contenido de la obligación de informar al titular en la recolección de datos que se reglamenta actualmente en el artículo 3.
- iii. Se requerirá consentimiento expreso del titular para efectuar tratamiento de datos personales, el que deberá, además, constar por escrito cuando se traten datos sensibles.
- iv. Aún cuando no se requiera autorización del titular, deberá informarse a éste conforme a las reglas generales. Se prescinde del consentimiento, pero no del conocimiento del titular.

v. Se invierte la carga de la prueba respecto a la calidad o corrección de la información y será el responsable del fichero quien procederá siempre a modificar, a menos que pruebe que dichos datos son correctos.

vi. Para cautelar el adecuado cumplimiento de las disposiciones relativas al tratamiento de datos personales, incluyendo el efectivo cumplimiento del derecho a ser informado, se contempla la existencia de una autoridad de control dotada de competencias y herramientas eficaces para:

- Dictar normativa sobre la materia de carácter general o particular respecto de las condiciones de legitimidad de un tratamiento de datos.
- Fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales.
- Adoptar medidas de resguardo para la adecuación del tratamiento de datos a las disposiciones de la ley.
- Sancionar los incumplimientos.
- Mantener un Registro Único Nacional de las Bases de Datos.
- Conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos.

Esta autoridad de control sería el Consejo para la Transparencia, creado por la Ley N° 20.285, que pasaría a denominarse Consejo para la Transparencia y la Protección de los Datos Personales.

Además, el proyecto contempla:

i. Establecer un catálogo pormenorizado de sanciones leves, graves y gravísimas específicas consistentes en multas o cancelación del registro.

Además, se establece un procedimiento sancionatorio que podrá iniciarse de oficio o por denuncia ante el Consejo para la Transparencia y Protección de Datos Personales, procediendo recurso de ilegalidad ante la Corte de Apelaciones.

ii. Establecer una regla de presunción de responsabilidad a favor del titular de los datos cuando se acredite la infracción a la ley.

iii. El Consejo para la Transparencia y Protección de Datos Personales llevará un Registro Único de Bancos de Datos, de carácter público, en el que constará:

- El responsable del banco de datos.
- El fundamento jurídico de la existencia del banco de datos.
- La finalidad del banco de datos.
- El domicilio del responsable del banco de datos.
- Los tipos de datos almacenados.
- La descripción del universo de personas que se comprende.
- Los destinatarios de los datos personales.

Concretamente, el derecho a ser informado se ve modificado en los siguientes puntos de acuerdo al proyecto:

1. Derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública.

El derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública se amplía, modificándose el artículo 3, en tanto se agrega que además de informar sobre el carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información, debe informarse sobre:

- a. Las consecuencias jurídicas de la negativa a responder las preguntas realizadas.
- b. La finalidad para la cual se está solicitando la información.
- c. Los destinatarios de los datos.
- d. La posibilidad de que estos datos sean comunicados a terceros.

2. Derecho a ser informado en toda solicitud de datos al propio titular.

El Proyecto de Ley agrega un artículo completo después del artículo 3, como artículo 3 bis, que se refiere al derecho a ser informado de modo expreso, preciso, claro e inequívoco en toda solicitud de datos.

Este derecho se extenderá a informar:

- a. De la existencia de un registro o banco de datos personales en el cual se consignará la información, identidad del titular del banco de datos y su domicilio, la finalidad de la recogida de datos y los destinatarios de la información.
- b. Del carácter obligatorio o facultativo de la entrega de datos personales que se le soliciten y las consecuencias de la entrega de los datos o de la negativa a suministrarlos.
- c. De los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo.
- d. Del derecho a revocar su autorización para el tratamiento de datos que le conciernen y las consecuencias de su revocación.
- e. De una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten.
- f. De la circunstancia de que los datos proporcionados vayan a formar parte de un registro o banco de datos de acceso público.

Cabe señalar que esta amplitud del derecho a ser informado se contempla para los casos de solicitud de datos, es decir, el órgano público, la persona jurídica privada o el

particular que pretendan realizar el tratamiento de datos requeriría los datos del propio afectado y no de terceras personas u otros registros.

3. Derecho a ser informado en la recogida de datos desde terceros.

Nos preguntamos qué sucede entonces con aquellos casos en que los datos no son recogidos del propio titular y que constituyen la gran mayoría de los casos de tratamiento de datos personales. Para esta hipótesis el proyecto contempla un inciso que señala:

“En los actos de recogida de datos desde terceros, deberá informarse al titular de datos de forma expresa, precisa, clara e inequívoca, por el responsable de la base de datos o su representante, dentro de los tres meses siguientes al momento del registro de los datos, de los datos objeto de tratamiento, la procedencia de los datos, así como de lo previsto en las letras a), c), d) y e) del inciso 1º del presente artículo”.

Este inciso es de inmensa importancia porque sienta el principio de conocimiento del tratamiento de datos personales a todo evento. Es decir, el titular de los datos no sólo tiene derecho a ser informado cuando los datos se recogen directamente de su persona, sino que este derecho se extiende a todos los casos en que la recogida de datos ha prescindido de su conocimiento lo que constituye realmente la regla general porque como ya hemos señalado, por el mismo carácter que trasciende a los bancos de datos, se trata de una actividad que normalmente se realiza a espaldas del afectado.

El titular deberá ser informado sobre los siguientes puntos:

a. De la existencia de un registro o banco de datos personales en el cual se consignará la información, identidad del titular del banco de datos y su domicilio, la finalidad de la recogida de datos y los destinatarios de la información.

- b. De los datos objeto de tratamiento.
- c. De la procedencia de los datos objeto de tratamiento.
- d. De los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo.
- e. Del derecho a revocar su autorización para el tratamiento de datos que le conciernen y las consecuencias de su revocación.
- f. De una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten.

El hecho que se fije un plazo específico para que el responsable del fichero informe es una garantía fundamental a la hora de instar al cumplimiento del derecho a informar, pues difícilmente se podrá cumplir un deber que no está sujeto a ninguna disposición específica que establezca la forma y momento del cumplimiento.

Este deber de información, no se aplicará en aquellos casos en que la ley exima del deber de forma expresa, cuando se efectuó tratamiento de datos con fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible.

4. Derecho a ser informado para autorizar y realizar el tratamiento de datos personales.

Examinando las falencias de la Ley N° 19.628 en cuanto establece que el derecho a ser informado no procede en los casos en que no se requiera consentimiento, que constituyen la regla general producto de las amplísimas excepciones, el proyecto ha realizado varias modificaciones en el artículo referido a la autorización del titular de los datos personales, planteando fundamentalmente que aun cuando no se requiera la autorización del titular, deberá informarse a éste conforme a las reglas generales, pues se puede prescindir del consentimiento pero nunca del conocimiento del titular.

Así se contempla en el último inciso que pretende introducir el proyecto:

“En todo caso, quienes realicen tratamiento de datos personales sin autorización del titular conforme a las disposiciones de este artículo, deberán informar del tratamiento de datos, en los términos del artículo 3 bis”.

A través de este inciso, se procede a realizar una separación nítida entre información y consentimiento. El hecho de requerirse consentimiento informado en ciertos casos específicos no implica que aquellos casos en que se pueda prescindir de esta manifestación de voluntad del titular de los datos, se pueda dejar también de informarlo sobre la existencia del registro, la identidad del titular, su domicilio, la finalidad de la recogida de datos, los derechos que le asisten y su ejercicio.

No obstante, se establece este deber de información de extensión generalizada, el proyecto pretende reducir la amplitud de las excepciones contempladas para solicitar autorización del titular de los datos para proceder al tratamiento de datos.

En primer lugar, se modifica el concepto de “fuentes accesibles al público”, sustituyéndose la expresión “de acceso no restringido o reservado a los solicitantes” por:

“Registros o recopilaciones de datos personales públicos o privados, cuyo acceso no se haya restringido o reservado sólo a los titulares e interesados en los datos personales que contiene, y que no hayan sido calificados como reservados o secretos en la normativa específica que les rija, tales como, la estadística de los censos; los listados telefónicos en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos profesionales que voluntariamente se hayan incorporado, consintiendo en el tratamiento público de sus datos, y que

contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, domicilio o residencia e indicación de su pertenencia al grupo; los diarios y boletines oficiales; y los medios de comunicación social”.

Además, se suprime del concepto de fuentes accesibles al público, los listados relativos a una categoría de personas que sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios pues como ya estudiamos, el reconocimiento de éstas como fuentes accesibles al público que no requieren autorización del titular de los datos para su tratamiento, legitima la actividad de marketing que debería estar claramente limitada.

La referencia a este tipo de registros de datos se reenvía al nuevo artículo 3 bis donde se dispone que estas comunicaciones comerciales cuando se dirijan al titular deben proveer información sobre el origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

5. Derecho a ser informado manifestado como derecho de acceso.

El deber del responsable del banco de datos se mantiene, en cuanto debe permitirle al titular de los datos, el acceso a éstos.

Este derecho de acceso se materializa en que el responsable del fichero, frente a la solicitud del titular de los datos, deberá informar.

- a. Sobre los datos relativos a su persona que constan en el fichero.
- b. Sobre la procedencia de tales datos.
- c. El destinatario de los datos.
- d. El propósito del almacenamiento de los datos.

e. La individualización de las personas y organismos a los cuales sus datos son transmitidos regularmente.

f. El titular de los datos puede exigir que se le informe sobre las evaluaciones y apreciaciones que sobre dicha información hayan sido comunicadas durante los últimos seis meses, así como los criterios de apreciación empleados, el nombre y dirección de la persona o entidad a quien se hayan comunicado los datos.

6. Derecho a ser informado manifestado como derecho de consulta frente al Registro Único Nacional de Bancos de Datos.

El proyecto hace extensible el ejercicio del derecho de información manifestado como derecho de consulta frente al Registro Único Nacional de Bancos de Datos, al que se podrá solicitar información sobre:

- a. La existencia de tratamiento de datos de carácter personal que pudieren afectarle.
- b. Las finalidades del tratamiento de datos personales.
- c. Todos los antecedentes necesarios para la identificación del responsable del tratamiento, consulta que podrá realizarse pública y gratuitamente.

El Registro Único Nacional de Bancos de Datos estará a cargo del órgano de control, es decir, del Consejo para la Transparencia y Protección de Datos Personales, de acuerdo a la nueva atribución que se le otorga en el artículo 33 bis a) de la Ley N° 20.285:

“Mantener un Registro Único Nacional de las Bases de Datos, sean estas de origen público o privado, en adelante, el Registro.

Este registro tendrá carácter público, y en él constará, respecto de cada banco de datos, su responsable, el fundamento jurídico de su

existencia, su finalidad, su domicilio, los tipos de datos almacenados, la descripción del universo de personas que comprende, y los destinatarios de los datos personales. Las particularidades de este registro y las normas sobre su implementación, serán establecidas por decreto supremo reglamentario del Ministerio Secretaría General de la Presidencia”.

Será deber de los responsables de los bancos de datos proporcionar los antecedentes mencionados, previamente al inicio de sus actividades, y comunicar cualquier cambio que se produzca en ellos dentro de los quince días desde que se verifique.

En casos excepcionales, el Consejo para la Transparencia y Protección de Datos Personales podrá disponer la simplificación o la omisión del registro, cuando se tratare de categorías de tratamientos que no afecten a los derechos y libertades de los titulares de la información, habida cuenta de los datos a que se refieren, y cuando el tratamiento se efectúe en el cumplimiento de disposiciones legales o reglamentarias.

7. Derecho a ser informado manifestado como derecho de modificación, eliminación y bloqueo.

El titular de los datos conserva la posibilidad de hacer valer sus derechos de modificación, eliminación y bloqueo cuando estos sean erróneos, inexactos, equívocos e incompletos.

Cabe señalar que la carga de la prueba se invierte. Antes el titular de los datos tenía que probar que los datos eran erróneos, inexactos, equívocos o incompletos, con la modificación a la ley, será el responsable del banco de datos quien deberá probar que los datos son correctos y que no procede su modificación, eliminación y bloqueo.

Limitaciones al derecho a ser informado en sus distintas manifestaciones.

Se mantienen las limitaciones del artículo 15 de la Ley N° 19.628.

Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.

El proyecto reemplaza el actual artículo 16 que consagra el derecho de hábeas data como recurso de reclamación por el siguiente precepto:

“La solicitud a que se refiere el inciso segundo del artículo 12 de esta ley, debe ser ejercida ante el responsable del banco de datos. Si éste no se pronunciare sobre la solicitud del requirente dentro de diez días hábiles siguientes, o veinte días hábiles tratándose de órganos de la administración del Estado, o la denegare injustificadamente, o tratándose de un órgano público no se encuentre amparado por la deberes de reserva derivados de la seguridad nacional, el titular de los datos tendrá derecho a recurrir ante el Consejo para la Transparencia y Protección de Datos Personales. Dicha reclamación se registrará por el procedimiento previsto en título V de esta ley”.

A través de este precepto se modifica en grandes términos el recurso de hábeas data que contemplaba la Ley N° 19.628 en su versión original:

- En cuanto al plazo para que el responsable del banco de datos se pronuncie sobre la solicitud, éste se extiende de dos días hábiles, como se contempla actualmente en la ley, a diez o veinte días hábiles, dependiendo si estamos ante un órgano privado o un órgano de la administración del Estado, respectivamente.
- El recurso se concede por las mismas causales anteriores, es decir, por denegar injustificadamente la información requerida o la solicitud de modificación, eliminación y bloqueo.

- El recurso no se ejerce ante los tribunales ordinarios de justicia, sino que el órgano competente para conocer de estas materias será el Consejo para la Transparencia y Protección de Datos Personales.

Simultáneamente al establecimiento del recurso de hábeas data reestructurado, el proyecto contempla un procedimiento administrativo para la aplicación de sanciones a los órganos públicos, personas jurídicas privadas y particulares que infrinjan la Ley N° 19.628, disponiendo 3 órdenes de sanciones de tipos leves, graves y gravísimas

Las nuevas disposiciones sancionan la infracción al derecho a ser informado que detenta el titular de los datos, estableciéndose que se considera:

i. Infracción leve:

- Infringir el deber de registro en el Registro Único Nacional de Bases de datos, cuando no sea constitutivo de infracción grave.
- Infringir el deber de información en la recogida de datos personales, cuando no sea constitutivo de infracción grave o gravísima.

ii. Infracción grave:

- Impedir u obstaculizar el ejercicio de los derechos de acceso y oposición.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan.
- No entregar la información solicitada por el Consejo para la Transparencia y Protección de Datos Personales en el ejercicio de sus funciones.

- No inscribir el registro o banco de datos personales en el Registro Único Nacional de Bases de Datos, habiendo sido requerido para ello por el Consejo para la Transparencia y Protección de Datos Personales.

- Infringir el deber de información al titular de los datos.

iii. Infracción gravísima:

- Incumplir las instrucciones impartidas por el Consejo para la Transparencia y Protección de Datos Personales sobre las condiciones de legitimidad de un tratamiento de datos.

- Realizar tratamiento de datos personales de forma ilegítima o con menosprecio de los principios y garantías que establece la ley, cuando ello derive en afectación a derechos fundamentales del titular de datos personales.

- No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

- No atender de forma sistemática el deber legal de información de la inclusión de datos de carácter personal en un registro o banco de datos.

Como vemos, el proyecto establece sanciones directas al incumplimiento del deber de información, como asimismo, sanciones generales por infracción a los principios que subyacen la legislación de protección a los derechos personales¹⁰⁹. Así, se instauran montos pecuniarios frente a las infracciones, los que fluctúan en los siguientes valores:

¹⁰⁹ Cabe señalar que el catalogo de infracciones es mucho más amplio y sólo se incluyeron las que regulaban directa o tangencialmente el derecho a ser informado del tratamiento de datos personales.

- Para infracciones leves: multas de hasta 200 UTM¹¹⁰, es decir, hasta alrededor de \$7.350.400.

- Para infracciones graves: multas de hasta 5.000 UTM, es decir, hasta alrededor de \$183.376.000.

- Para infracciones gravísimas: multas de hasta 10.000 UTM, es decir, hasta alrededor de \$367.520.000.

Estos montos superan ampliamente las multas establecidas de acuerdo a la legislación actual. Las nuevas multas pueden ser disuasivos reales a la hora de cumplir la legislación, pues ya no será más eficiente pagar las sanciones que adecuarse a la ley. Sin embargo, el monto específico de la multa quedará a la determinación del Consejo de Transparencia y Protección de Datos Personales que decidirá apreciando la gravedad, las consecuencias del hecho, el volumen del tratamiento efectuado, la capacidad económica del infractor y si este hubiera cometido otras infracciones de cualquier naturaleza en los últimos 24 meses.

Este procedimiento administrativo podrá iniciarse de oficio por el Consejo para la Transparencia y Protección de Datos Personales o por denuncia presentada por el particular afectado. Con el Proyecto de Ley se resolvería el problema que presenta la legislación actual, que al no establecer la existencia de un registro de las bases de datos particulares, torna en impracticable las acciones de reclamación y sancionatorias. Actualmente es totalmente factible que el individuo nunca se entere sobre el tratamiento de sus datos personales.

Aún así, si el titular quiere ejercer acción indemnizatoria, está todavía se contempla pero se ha dispuesto en un nuevo artículo 27 que señala el derecho a ser indemnizado por el responsable del banco de datos y, solidariamente, por los cesionarios de dichos datos. Asimismo, se establece presunción legal de responsabilidad, si existe infracción

¹¹⁰ UTM calculada de acuerdo al mes de marzo de 2010.

a las normas de la Ley N° 19.628, invirtiéndose la carga de la prueba sobre el responsable del fichero, quien debe probar que ha dado cumplimiento a las disposiciones legales.

4.2. Proyecto de Ley sobre deuda positiva y negativa de los chilenos.

El 12 de mayo de 2009, causó gran revuelo mediático la reunión que sostuvo la Subsecretaría de Hacienda, María Olivia Recart, con los integrantes de la Comisión de Economía de la Cámara de Diputados para darles a conocer los alcances del nuevo proyecto de información comercial positiva.

El proyecto vino a sustituir el texto de los proyectos de ley presentados por los boletines 5309-03 y 5356-07. El proyecto de boletín 5356 ingresó al Congreso el 3 de octubre de 2007 y planteaba la modificación de la Ley N° 19.628, en términos de establecer la obligación del responsable del banco de datos, de informar al “propietario” acerca de éstos, y a quién le ha sido entregada dicha información.

En efecto, este proyecto detecta que para los efectos de resguardar el orden público económico resulta indispensable un sistema adecuado y moderno de publicación de antecedentes sobre mora y protestos de ciertos documentos mercantiles, pues se reconoce la seguridad otorgada al sistema comercial. No obstante, se percibe que en la actualidad existe un desconocimiento por parte de las personas respecto a quienes son las empresas dedicadas al rubro del tratamiento y almacenamiento de datos personales, aparte de DICOM y la Cámara de Comercio, que son las más conocidas.

Así, señala el proyecto de boletín N° 5356-07:

“La mayoría de las personas poseen tarjetas de crédito, distintas a las bancarias, a modo de ejemplo: tarjetas de farmacias, tiendas comerciales, zapaterías etc. Al momento de acceder a este dinero plástico deben firmar un contrato donde autorizan que sus

antecedentes sean almacenados en un banco de datos, pero todos sabemos que contratos tan extensos y detallados no son leídos en su gran mayoría por la gente, son contratos de adhesión donde no existe ninguna posibilidad de negociar alguna cláusula”.

En este contexto se reconoce, reafirmando el principio de transparencia, que las personas que se dediquen al rubro de tratamiento de datos personales, deben informar, una vez al año, a los "propietarios" sobre la información que poseen de su persona, el propósito de su almacenamiento y quienes han consultado por sus datos.

Así, se pretendía que el artículo 12 figurará en los siguientes términos:

“Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. Para estos efectos el responsable del banco de datos deberá comunicar una vez al año a dicha persona esta información, la cual le será enviada al domicilio que tenga registrado en dicho registro de datos personales”.

El 3 de octubre de 2007 se dio cuenta del proyecto y se ordenó su paso a la Comisión de Constitución, Legislación y Justicia. Luego, el 9 de abril de 2008, la Comisión de Economía solicitó que se le remitiera el proyecto, devolviéndolo transcurrido más de un año con un oficio que indicaba su sustitución por el nuevo proyecto N° 293-357.

El nuevo proyecto abarca una extensión de contenido mucho más amplia y diametralmente distinta que la de sus proyectos de origen, disponiendo su pretensión de derogar completamente el título III de la actual Ley N° 19.628 y abordar sólo los datos económicos o información comercial, mientras que el resto de las bases de

datos, serían abordadas en el Proyecto de Ley N° 68 7-356, al que hicimos referencia anteriormente.

El Proyecto de Ley reconoce cuatro ejes estructurantes:

- i. Se refuerzan los derechos de los titulares de los datos.
- ii. Se amplía la información relativa a obligaciones económicas disponible en el mercado financiero, para que además de los datos sobre deudas morosas que hoy existe, también se registre el buen comportamiento de pago de las personas.
- iii. Se introducen mecanismos de control de calidad de los datos.
- iv. Se crea una instancia administrativa para regular, fiscalizar y sancionar a los agentes y ordenar el mercado de la información comercial.

El proyecto se estructura sobre la premisa de que aquella información concerniente a las obligaciones económicas y la conducta de pago de las personas naturales y jurídicas es esencial para que el mercado de crédito funcione adecuada y eficientemente.

En este sentido, los registros de datos comerciales permitirían atenuar las asimetrías que existen entre acreedores y deudores potenciales, viabilizando el acceso de las personas naturales y las pequeñas y medianas empresas al financiamiento. Simultáneamente se disminuye el riesgo de sobreendeudamiento y el grado de incumplimiento en la economía.

El problema fundamental consistiría en la dificultad de las entidades financieras para seleccionar su cartera de clientes. En efecto, como los acreedores están imposibilitados de discriminar adecuadamente entre un mejor o peor pagador, atendida la falta de información, el costo de los créditos se establecerá sobre la base de promedios que benefician a los deudores más riesgosos y perjudican a los

cumplidores, pues los primeros no dimensionan íntegramente las consecuencias que se derivan de sus incumplimientos y eligen sobreendeudarse.

En este contexto, se concluye que poseer mayor disponibilidad de información sobre el potencial deudor, reduciría estos riesgos e incentivaría a dar cabal cumplimiento a los compromisos adquiridos con las entidades financieras. De aquí, que se afirme que la información económica de las personas genera efectos de relevancia social y no es posible considerar a estos datos como datos de ámbito exclusivo de la vida privada.

Para que las entidades financieras sean capaces de evaluar eficientemente el nivel de riesgo sería igual de importante la información sobre deuda morosa y sobre deuda al día de los futuros acreedores, y no sólo respecto a esta misma entidad financiera, sino también de otras de la misma categoría.

Hoy en día el sistema de información comercial no posee una regulación unificada, sustentándose en tres sistemas particulares:

a) El Boletín de Información Comercial (BIC): está constituido por los protestos de cheques, letras y pagarés que deben informar los bancos y los notarios a la Cámara de Comercio de Santiago, de forma obligatoria. El BIC actúa como centralizador del sistema.

b) INFOCOM: es un banco de datos que comercializa la Cámara de Comercio y que contiene información sobre cuotas morosas que no se han protestado y que son discrecionalmente manifestadas por el comercio, los bancos y otros acreedores. En esencia, compila la información negativa que se genera directamente del sistema de casas comerciales –es decir, las cuotas morosas de créditos y tarjetas de crédito- que se encuentran sujetas a un modelo voluntario de envío por parte de los acreedores¹¹¹.

¹¹¹ ORTIZ, Claudio, La protección de datos personales y la información comercial, en obra colectiva Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?, Santiago, Serie Políticas Públicas, 2009, Pág. 26.

c) Estado de deudores: es un registro público que lleva la Superintendencia de Bancos e Instituciones Financieras, el cual no sólo contiene información sobre deuda morosa, sino también información al día de los clientes bancarios, estableciéndose por la Ley General de Bancos que esta información no puede comunicarse a otros agentes económicos distintos de los bancos, sin que medie el consentimiento de deudor. La distribuidora de información crediticia (ABIF) permite que el Sistema Nacional de Comunicaciones Financieras (SINACOFI) pueda acceder al estado de deudores de las instituciones financieras para el cumplimiento de sus finalidades de administración, operación y desarrollo de una red electrónica capaz de apoyar la acción comercial operativa de las instituciones financieras.

SINACOFI es uno de los cuatro buros de crédito que se desempeñan como empresas distribuidoras finales de información comercial, sin embargo, ocupa sólo un 15% de participación del mercado, siendo superada ampliamente por DICOM que detenta un 70% del mercado. Estas empresas, a través de licencias de uso con la Cámara de Comercio de Santiago, obtienen los datos del Boletín de Información Comercial, poniéndolos a disposición de los interesados.

El Proyecto de Ley detecta que el problema más importante de la industria de la información comercial en Chile consiste en la inexistencia de un sistema de regulación adecuado. Los controles de calidad y veracidad de los datos, las normas de seguridad para proteger la información, los plazos y formatos de envío de la información, entre otros problemas, son materias establecidas por los mismos agentes del mercado y con un alto rango de desconocimiento por parte de la sociedad. A esto se suma la falta de una entidad supervisora que fiscalice el funcionamiento de este mercado y la carencia de una vía expedita que permita el ejercicio de los derechos de los consumidores.

La temática más relevante para este estudio, en cuanto a las debilidades de la industria de la información, consiste en que el actual sistema de información comercial no garantiza la protección al titular de los datos, problema que desde el punto de vista del mercado puede afectar la calidad de la información circulante. Entre los inconvenientes

de la Ley N° 19.628 se encuentra la carencia de procedimientos claros para corregir errores, para acceder a la información propia y para conocer con qué fines y quiénes la están utilizando.

La actual Ley de Protección a la Vida Privada enlista los datos personales de carácter económico, financiero, bancario o comercial entre datos que provienen o se recolectan de fuentes accesibles al público y que no requieren autorización del titular de los datos para ser tratados, tal como se dispone en el artículo 4 de la actual ley. Como ya señalamos, esta excepción a realizar tratamiento sin autorización, conlleva al entendimiento de que tampoco debe informarse sobre el tratamiento y este puede realizarse con total prescindencia del conocimiento del particular. En este sentido, pese a que el artículo 12 disponga el derecho de acceso, modificación, eliminación y bloqueo, este se obstaculiza ostensiblemente por no contemplarse el requisito de informar de modo expreso, preciso, claro e inequívoco, al afectado en el tratamiento de datos personales.

En el título III de la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario y comercial se señala que los responsables de los registros de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando:

- Éstas consten en letras de cambio y pagarés protestados.
- Éstas consten en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa.
- Cuando se han incumplido obligaciones derivadas de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

- Se trate de otras obligaciones en dinero que por Decreto Supremo el Presidente de la República haya determinado como comunicables.

Es un tema de entendimiento general que la información negativa es bastante acotada y se justifica por sí sola por el hecho de que su promoción sin el consentimiento del titular tiene por objetivo ayudar a prevenir al mercado sobre aquellas personas que por diversas razones tienen conductas comerciales desordenadas¹¹². Sin embargo, respecto a todas estas obligaciones tratadas en bancos de datos, actualmente no se tiene tampoco un claro derecho de información¹¹³ y normalmente el titular de los datos podrá advertir carencia de fundamento legal, caducidad, error, inexactitud o equivocidad porque se le niega el ejercicio de determinado derecho o facultad.

En varios de los fallos dictados por nuestros Tribunales Superiores de Justicia que hacen aplicación a la Ley N° 19.628, a raíz de acciones presentadas contra determinados órganos y DICOM por comunicación de deudas inexistentes, ya pagadas o deudas que no corresponden a obligaciones de carácter económico, financiero, bancario o comercial, queda en evidencia que los particulares se han enterado de la consignación de estos datos porque se les deniegan solicitudes de créditos, pagos con cheques y participación en licitaciones, lo que implica que ya se han registrado perjuicios de algún tipo por la carencia de información cierta y veraz¹¹⁴.

¹¹² ORTIZ, Claudio, La protección de datos personales y la información comercial, en obra colectiva Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?, Santiago, Serie Políticas Públicas, 2009, Pág. 26.

¹¹³ Ya advertimos que prescindir del consentimiento no implica prescindir del conocimiento del titular ejercido a través del derecho a ser informado.

¹¹⁴ (1) Corte Suprema, 14 de octubre de 2008, Luis Gonzaga García con Scotiabank, “al pretender hacer un pago con cheque sobre su cuenta corriente, en otro banco, se le informó que no podía hacerlo porque aparecía como deudor moroso en los registros de la empresa DICOM”. (2) Corte Suprema, 19 de noviembre de 2007, Gustavo Flores Muñoz con Dirección Regional del Servicio de Tesorería de Temuco, “concurrió a una casa comercial y al pretender obtener una tarjeta de crédito, le fue rechazada por registrar una anotación de deuda”. (3) Corte de Apelaciones de Concepción, 31 de julio de 2007, Gabriel Alfonso Da Fonseca Barría con Tesorero Provincial de Bío Bío, “cuando intentó cancelar una compra de repuestos con un cheque de la cuenta corriente de la sociedad que representa, le fue rechazado por registrar deuda fiscal morosa”. (4) Corte Suprema, 24 de mayo de 2007, Pedro Lepe Ramírez con Dirección Regional del Servicio de Tesorerías, “el señor Lepe al intentar realizar una compra y pagar con un cheque de su cuenta corriente personal, le fue rechazado tal documento”. (5) Corte de Apelaciones La Serena, 22 de marzo

En vista de la serie de debilidades radicadas en la actual Ley de Protección a la Vida Privada, la indicación sustitutiva pretende realizar variados cambios que afectan al derecho a ser informado:

i. Ampliación de los titulares de los datos: las personas jurídicas también podrían ser titulares de datos y podrían reivindicar su protección de forma equivalente a las personas naturales.

ii. Extensión del concepto de información comercial: además de la información sobre obligaciones de carácter económico, financiero, bancario o comercial de las características que señalamos en los párrafos precedentes, la indicación sustitutiva amplía el tipo de obligaciones que debe comunicarse, incluyendo también, bajo ciertas condiciones, las deudas al día de las personas naturales y jurídicas.

iii. Ampliación de las instituciones obligadas a informar: las entidades obligadas a reportar periódicamente los datos de obligaciones económicas, abarcarán a las Bancos, las Casas Comerciales, las Compañías de Seguros, las Cooperativas, las Cajas de Compensación, las Empresas de Leasing y las de Factoring, así como la Tesorería General de la República, en lo que respecta a deudas tributarias demandadas.

de 2007, Orlando López Sánchez con ADT Security Services, "Luego de tener distintos inconvenientes comerciales el señor López Sánchez tomó conocimiento que aparecía en el Boletín Comercial".(6) Corte Suprema, 28 de marzo de 2007, Jorge Rafael Rojas Figueroa con Tesorería Regional de la Novena Región, "A raíz de la comunicación enviada por Tesorería se le suspendió de la página Chilecompras y por lo tanto no tiene acceso a ninguna licitación pública". (7) Corte Suprema, 15 de febrero de 2007, Gabriel Ernesto Vásquez Albarracín, "al intentar consolidar sus deudas en una institución financiera, se le indicó que ello no sería posible, por figurar como deudor de la Tesorería General de la República". (8) Corte Suprema, 2 de octubre de 2006, Raúl Sube Guzmán con Tesorería Provincial de Osorno, "Concurrió a la oficina de Osorno del Banco del Estado de Chile, a objeto de solicitar un crédito o mutuo con dinero con el fin de desarrollar sus actividades comerciales. Al efectuarse un estudio de sus antecedentes comerciales y financieros se le indicó que no se le podía otorgar el referido préstamo de dinero y, por consiguiente, se le rechazaba la operación crediticia por registrar una deuda en DICOM para con la Tesorería General de la República".

iv. Instauración de un Registro Central de Obligaciones Económicas (RECOE): el proyecto establece la creación de un banco de datos oficial licitado, en que se registrarían todos los datos provenientes de obligaciones económicas con la finalidad de conservar, consolidar y estandarizar la información sobre deuda morosa y al día, la que deberá ser remitida por los aportantes, de acuerdo a las instrucciones que dicte la Superintendencia de Bancos e Instituciones Financieras.

v. Consentimiento de los titulares de los datos: se exigirá el consentimiento del titular para aquellos casos en que se desee comunicar deuda al día a cualquier persona o entidad que requiera utilizar esta información para evaluar el riesgo crediticio u otro fin autorizado por la ley.

vi. Organismo fiscalizador: las facultades normativas, reguladoras y sancionatorias en materia de información comercial serán de competencia de la Superintendencia de Bancos e Instituciones Financieras, radicándose en ella la función de vigilar y fiscalizar que los aportantes de información, el Registro Central de Obligaciones Económicas y las Distribuidoras cumplan con la normativa vigente, los reglamentos e instrucciones que se le impartan.

vii. Fortalecimiento del derecho de información y de acceso a los datos propios: este tema es uno de los más relevantes pues pese a que la indicación sustitutiva amplía bastante la información económica circulante y las entidades obligadas a informar, se pretende dotar al sistema de protección de datos de nuevos mecanismos de información y acceso, llenándose el vacío normativo actual que provoca la limitación de los derechos económicos de las personas. En efecto, se establece que los titulares de los datos tendrán el derecho a ser informados por los aportantes de información sobre los siguientes puntos:

- Propósito del tratamiento de información.
- Contenido del banco de datos.

- Destinatarios y cesionarios de los datos de obligaciones económicas.
- Si su historial ha sido utilizado para tomar una decisión adversa o favorable.

Además, todo titular podrá acceder a sus datos existentes en el Registro Central de Obligaciones Económicas, gratuitamente, una vez al año. Se estima que la regulación de este derecho frente al registro, las distribuidoras y los titulares, deberá ser complementado por un reglamento.

viii. Perfeccionamiento del derecho de rectificación y cancelación de datos: el proyecto estipula un procedimiento administrativo, distinto al contemplado para otros tipos de datos, para rectificar y cancelar datos.

El afectado tiene derecho a agregar una nota en el registro, haciendo la observación de que el dato está siendo impugnado. Mientras, en caso de error, se establecerá un procedimiento expedito para que todos los responsables de bases de datos donde se consigne esta información, rectifiquen el error.

Si el afectado no queda satisfecho con la respuesta entregada por el responsable del banco de datos, puede recurrir al Consejo para la Transparencia y Protección de Datos Personales, sin perjuicio, de que se conserve la facultad de recurrir ante los Tribunales Ordinarios de Justicia.

ix. Regulación de las obligaciones de todos los suministradores de datos de obligaciones económicas: los distribuidores de información, para desenvolverse como tales y acceder a la información del Registro Central de Obligaciones Económicas deben constituirse como sociedades y registrarse ante la Superintendencia de Bancos e Instituciones Financieras. Además, para permanecer en la nómina de entidades autorizadas deben adoptar medidas de seguridad y realizar periódicamente auditorías externas que cautelen el adecuado tratamiento de la información.

Concretamente, el derecho a ser informado se ve modificado en los siguientes términos de acuerdo al proyecto:

1. Derecho a que se registren, comuniquen y difundan datos personales fidedignos, veraces y actualizados.

En el párrafo dos del título I que trata las disposiciones comunes, la indicación sustitutiva señala que las actividades de registro, comunicación y difusión de datos personales referentes a obligaciones económicas deberán ser veraces, fidedignas y actualizadas, aspectos que deberán ser garantizados por las entidades de fiscalización, las que verificarán que las entidades fiscalizadas cumplan los siguientes deberes:

- i. Adoptar medidas técnicas y organizativas que garanticen que la información objeto del tratamiento de datos sea cierta, actualizada, completa y que no induzca a error o engaño.
- ii. Establecer procedimientos de validación, de actualización periódica y de rectificación de la información en conformidad a las disposiciones de la indicación sustitutiva, sus reglamentos y las normas impartidas por la Superintendencia de Bancos e Instituciones Financieras y demás autoridades competentes.

2. Derecho a ser informado por los aportantes a solicitud escrita del titular de los datos.

Este es el primer derecho contemplado en el título II que establece normas relativas a los titulares de datos de obligaciones económicas y dispone que todo titular tiene derecho a ser informado por los aportantes¹¹⁵, sin cargo alguno, cuando así lo solicite por escrito, sobre lo siguiente:

¹¹⁵ De acuerdo al artículo 2 letra f) de la indicación sustitutiva son aportantes, las personas naturales y jurídicas obligadas a reportar periódicamente al registro los datos de obligaciones económicas que esta ley y sus reglamentos señalen. Tendrán el carácter de aportantes:

- Las personas naturales o jurídicas que sean acreedores en forma habitual de operaciones de crédito de dinero en los términos definidos en la ley N° 18.010, y que registren un monto anual promedio de préstamos igual o superior al equivalente de UF 100.000.
- Los emisores y operadores de tarjetas de crédito bancarias o no bancarias.

- a. La confirmación de la existencia o inexistencia del tratamiento de datos que le concierne.
- b. El contenido de la información, que incluye entre otros, la individualización del Titular y del aportante, los montos de las obligaciones económicas a que se refieren y la fecha en que se contrajo la obligación.
- c. El propósito del tratamiento de los datos.
- d. Los destinatarios y cesionarios de los datos, distintos del registro, de los últimos doce meses.
- e. Si su historial ha sido utilizado para tomar una decisión adversa o favorable.
- f. De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

Cabe señalar, que este derecho a ser informado no difiere al contemplado actualmente en el artículo 12 de la Ley de Protección a la Vida Privada, pues su ejercicio está condicionado a la solicitud del titular de los datos personales. Claramente este derecho se aparta del sistema que se espera consagrar con la modificación a la Ley N° 19.628, propuesta a través del mensaje 687-356, y que establece que cuando se recojan datos

-
- Las personas naturales o jurídicas que efectúen operaciones de Leasing.
 - La Tesorería General de la República.
 - Los Notarios Públicos en lo relativo a letras de cambio y pagarés protestados.
 - Los bancos deberán informar, además de las obligaciones indicadas en el inciso anterior, los cheques protestados.
 - Los aportantes establecidos mediante Decreto Supremo y que cumplan copulativamente los siguientes requisitos: (1) que sean acreedores de una operación de crédito de dinero; (2) que las obligaciones de operaciones de crédito de dinero estén sustentadas en instrumentos de pago o de crédito válidamente emitidos; (3) que en los instrumentos indicados en el numeral anterior, conste el consentimiento expreso del deudor y su fecha de vencimiento.

de terceros se debe informar precisa, clara e inequívocamente, dentro de los tres meses siguientes al momento del registro de los datos objeto de tratamiento, su procedencia, entre otros, es decir, el deber de información pesa sobre el titular del registro.

A través de la modificación sustitutiva pareciera que se exime del deber de información de oficio, a un corto plazo desde la recogida, y éste sólo se contempla como un derecho ejercido esencialmente a solicitud del interesado. Pareciera que esta decisión legislativa se justifica porque el registro de información negativa tiene por finalidad prevenir al mercado sobre aquellas personas negligentes que no cumplen sus obligaciones económicas contraídas, las que obviamente estarán en pleno conocimiento sobre sus incumplimientos.

Sin embargo, cabe advertir que el derecho de protección de datos se desarrolla en la medida que se produzcan disconformidades entre las informaciones registradas en los bancos de datos y la información real del titular de los datos, o bien, cuando simplemente se asimilen determinados datos como de fuente accesible al público y realmente no lo son. Esta situación queda en evidencia al observar la jurisprudencia de los Tribunales Superiores de Justicia donde se observa, nuevamente, que gran parte de los recurrentes presenta acciones porque se les consigna como incumplidores ya que se registran informaciones erróneas, inexactas, equivocadas, incompletas, caducas o se publican datos a los que no les corresponde este tratamiento¹¹⁶.

¹¹⁶ Corte Suprema, 14 de octubre de 2008, Luis Gonzaga García Ortiz con Scotiabank, "Las dos cuotas de 2, 07 U.F. declaradas vencidas y morosas e informadas al Boletín Comercial, no corresponden a cuotas del dividendo pactado en la escritura de 28 de noviembre de 1997; el demandado sufrió un detrimento o menoscabo psicológico a raíz de la publicación en DICOM de una calidad de deudor inexistente". (2) Corte de Apelaciones de Santiago, 28 de abril de 2008, Enrique Troncoso Bruzzone con DICOM EQUIFAX S.A., "La deuda publicada en DICOM no emana de ninguno de los títulos a los que la Ley N° 19.628 se refiere en su artículo 17...DICOM ha incurrido en un acto ilegal, puesto que ha hecho una publicación en sus registros no autorizada por ley". (3) Corte Suprema, 4 de marzo de 2008, Alejandro Ramírez Valdivia con Dirección del Trabajo y Otro, "La comunicación de los datos materia del presente recurso de practicó después de transcurridos cinco años desde que la última obligación a que alude el fundamento sexto se hizo exigible, de lo que resulta que se ha vulnerado en la especie la prohibición establecida en el inciso primero del artículo 18 de la Ley N° 19.628". (4) Corte Suprema, 31 de diciembre de 2007, Claudia Haussmann Hevia con DICOM EQUIFAX S.A. e Interciti S.A., "Tanto la actuación de Interciti al enviar información de morosidad a DICOM EQUIFAX, hoy EQUIFAX CHILE S.A., para que fuera ingresada al sistema consolidado de morosidad

(SICOM), como la de EQUIFAX CHILE S.A., al incorporar información al sistema indicado, antes de que ellos fuera publicado en el Boletín Comercial, resulta ilegal". (5) Corte Suprema, 19 de Noviembre de 2007, Gustavo Flores Muñoz con Dirección Regional del Servicio de Tesorería de Temuco, "Resulta ilegal el acto imputado a la recurrida, consistente en remitir y autorizar la publicación por parte de la empresa DICOM, de la situación de morosidad referida en la letra a) del motivo quinto, que afecta al recurrente". (6) Corte de Apelaciones de Concepción, 31 de julio de 2007, Gabriel Alfonso Da Fonseca Barría con Tesorero Provincial de Bío Bío, "Los organismos públicos no pueden comunicar información de datos personales que verse sobre obligaciones no incluidas en la enumeración contenida en el artículo de datos personales que verse sobre obligaciones no incluidas en la enumeración contenida en el artículo 17 de la Ley N° 19.628, salvo que cuenten con el consentimiento del titular, y respecto de la situación que nos convoca, fuerza es concluir que la enumeración referida, que es taxativa como se dijo, no incluye los giros de impuestos como los informados por el recurrido DICOM respecto de los recurrentes". (7) Corte Suprema, 2 de octubre de 2006, Raúl Sube Guzmán con Tesorería Provincial de Osorno, "El Servicio de Tesorerías sólo puede informar sin restricciones datos de carácter personal en la medida que éstos versen sobre algunas de las obligaciones a que se refiere el artículo 17 de la citada ley, por cuanto así lo ordena el artículo 20 del mismo cuerpo legal, y no aquellos otros que se originan en obligaciones provenientes de impuestos, multas y de carácter tributario, en cuyo caso sí es preciso que el afectado manifieste su consentimiento. (8) Corte Suprema, 26 de julio de 2001, Gonzalo Baeza Ovalle con Corpbanca y DICOM, "Al haberse pagado por el actor, en el mes de marzo de ese año, como se ha dicho, el total de la deuda que a la sazón mantenía, no le era lícito a la mencionada recurrida enviar a protesto tal documento, con posterioridad a dicho pago, esto es, el 13 de abril del 2000, por lo que al no entenderlo así Corpbanca incurrió en un acto arbitrario". (9) Corte Suprema, 15 de febrero de 2007, Gabriel Ernesto Vásquez Albarracín con Tesorería Regional de Magallanes y Antártica Chilena, "Según lo admite la recurrida, ha informado a DICOM S.A. la deuda que el recurrente mantiene con el Fisco de Chile, originada en Impuesto al Valor Agregado y multa, deuda que no consta en ninguno de los instrumentos mercantiles ya referidos, ni corresponde a alguna de las obligaciones también relacionadas en el fundamento anterior, por lo tanto, para dar a conocerla públicamente, debió contar con el consentimiento del titular, lo que ciertamente no ha ocurrido". (10) Corte Suprema, 28 de marzo de 2007, Jorge Rafael Rojas Figueroa con Tesorería Regional de la Novena Región, "El Servicio de Tesorería sólo puede informar, sin restricciones, datos de carácter personal en la medida que éstos versen sobre algunas de las obligaciones a que se refiere el artículo 17 de la citada ley, por cuanto así lo ordena el artículo 20 del mismo cuerpo legal, y no aquellos que se originen en obligaciones provenientes de impuestos, multas y de carácter tributario, en cuyo caso se requiere que el afectado manifieste su consentimiento. La recurrida, al ordenar la publicación de la deuda del recurrente en el sitio web Chileproveedores, incurrió en una conducta ilegal". (11) Corte de Apelaciones, 22 de marzo de 2007, Orlando López Sánchez con ADT Security Services y DICOM S.A., "no resulta prudente ni racional, publicar en un sistema de datos de morosos, a quien no haya pagado una o más facturas, que no constituye un instrumento que acredite una deuda indubitada". (12) Corte Suprema, 24 de mayo de 2007, Pedro Lepe Ramírez con Dirección Regional de Tesorería de Concepción, "La recurrida, ha actuado en forma arbitraria e ilegal, vulnerando el derecho del recurrente al respeto y protección a su vida privada, garantizado en el artículo 19 N° 4 de la Constitución Política de Chile, al incluir en DICOM los antecedentes relacionados con las deudas tributarias cobradas al recurrente, reclamadas por éste y cuya resolución se encuentra pendiente en los Tribunales de Justicia". (13) Corte Suprema, 23 de julio de 2007, Guard Service Sistemas de Seguridad y Servicios Limitada con Inspección Comunal del Trabajo de Viña del Mar, "No corresponde que la Inspección del Trabajo envíe información aludida a DICOM por resultar ello improcedente, no se comparte lo decidido en cuanto a disponer que la recurrida deba cerciorarse previamente que el incumplimiento haya ocurrido y que consecuentemente proceda su inclusión en el registro por cuanto como ya se dijo tal información no puede ser incluida". (14) Corte Suprema, 7 de junio de 2007, Francisco Javier Larenas Sanhueza con Dirección del Trabajo y DICOM S.A., "La Dirección de Trabajo sólo puede informar sin restricciones datos de carácter personal en la medida que éstos versen sobre algunas de las obligaciones a que se refiere el artículo 17 de la citada ley, por cuanto así lo ordena el artículo 20 del mismo cuerpo legal, y no aquellos otros que se originan en obligaciones provenientes de cotizaciones previsionales, en cuyo caso sí es preciso que el afectado manifieste su consentimiento, lo que no ha ocurrido en la especie". (15) Corte Suprema, 22 de enero de 2007, Comercial Insumex con Tesorero General de la República, "La recurrida al ordenar la publicación de la deuda de la empresa recurrente en el Boletín Comercial, incurrió en una conducta ilegal y arbitraria".

Cabe advertir que estas situaciones se producen en nuestro actual sistema que sólo permite tratar, sin consentimiento informado del titular, datos económicos, financieros, bancarios o comerciales que se recolecten de fuentes accesibles al público y que se encuadren con las obligaciones del artículo 17 de la Ley de Protección a la Vida Privada. El problema, es que en la práctica se suelen agregar a los contratos de adhesión, que suscriben mecánicamente muchos consumidores, cláusulas que consienten en el tratamiento de datos personales de otros tipos de obligaciones, a fin de ser consignadas en un banco de datos, ampliándose enormemente el catálogo de información financiera que podrá ser de público acceso.

Desde esta óptica los cambios que propone la modificación sustitutiva son preocupantes, ya que avalará el tratamiento de un sinnúmero de datos personales económicos, financieros, bancarios y comerciales, sobrepasando en inusitadas dimensiones el volumen de la actual información circulante de esta categoría. Imaginemos como afectará la ampliación de las instituciones obligadas a informar, pues se instará a que periódicamente las obligaciones económicas sean reportadas por los Bancos, las Casas Comerciales, las Compañías de Seguros, las Cooperativas, las Cajas de Compensación, las Empresas de Leasing, las de Factoring y la Tesorería General de la República.

A esto, debemos agregarle el fundamento central de la modificación sustitutiva, que descansa en la extensión del concepto de información comercial que incluirá, bajo ciertas condiciones, las deudas al día de las personas naturales y jurídicas, caso en el cual tampoco se requerirá el consentimiento del titular de los datos para su recolección y comunicación.

Por lo tanto, si el Proyecto de ley de información positiva de los chilenos llegará a aprobarse se unificarán las bases de datos de deudores del *retail* y de la banca, configurándose de esta manera un historial de cada individuo, en su rol de consumidor, en base a los registros de las casas comerciales, las instituciones financieras y los otros actores del mercado económico que ya mencionamos, cuyo contenido no sólo

abordará la información económica negativa, sino que también la información positiva de los individuos, la que compilada, se consignará en el Registro Central de Obligaciones Económicas.

3. Derecho a ser informado manifestado como derecho de acceso.

De acuerdo al artículo 14 que consagra la modificación sustitutiva, el titular de los datos económicos, financieros, bancarios o comerciales tendrá derecho a acceder a sus datos de obligaciones económicas que son objeto de tratamiento por parte de las entidades fiscalizadas.

Sin embargo, este derecho de acceso estará condicionado a las restricciones establecidas en la presente ley y sus reglamentos:

i. Derecho de acceso gratuito una vez al año: el titular tendrá derecho a solicitar y recibir gratuitamente del administrador del Registro Central de Obligaciones Económicas, a través de cualquier distribuidora u otro canal que determine la Superintendencia de Bancos e Instituciones Financieras, un reporte anual en conformidad a las disposiciones de la modificación sustitutiva, sus reglamentos y la normativa que imparta la autoridad competente.

El contenido del reporte anual será únicamente el siguiente:

- Identificación de los acreedores del titular.
- Todo otro tipo de información relativa a los acreedores del titular que se encuentre disponible en el Registro Central de Obligaciones Económicas.

ii. Derecho de acceso gratuito permanente: el titular de los datos tendrá derecho a tomar conocimiento, gratuitamente y en cualquier época, únicamente de la identidad de sus acreedores incluidos en el Registro Central de Obligaciones Económicas.

iii. Derecho de acceso previo pago de tarifa permanente: el titular tendrá derecho, previo pago de una tarifa, a:

- Conocer los datos que sobre él existan en el Registro.
- Recibir informes comerciales de las distribuidoras.
- Conocer quiénes han recibido dicha información en los últimos doce meses.

Por lo tanto, si el titular de los datos quisiera solicitar información sobre los datos relativos a su persona que constan en el fichero, que vendría siendo el punto más importante para ejercer un eventual derecho de modificación, eliminación y bloqueo de datos, deberá siempre pagar una tarifa. Para ejercitar su derecho de acceso gratuitamente deberá recurrir a los aportantes de acuerdo al derecho que contendría el artículo 13 y que señalamos en el punto 2. que opera a solicitud del afectado.

Cabe subrayar que el derecho de acceso no se ejercería directamente contra el Registro Central de Obligaciones Económicas, sino a través de la figura de las distribuidoras¹¹⁷, a las que se les atribuyen una serie de obligaciones vinculadas al derecho de información y acceso del titular, las que se detallan en el artículo 43 del Proyecto de Ley:

i. Recibir las solicitudes de reporte anual efectuadas por el titular, previa autenticación de éste, y luego remitirlas al administrador del registro, en conformidad al inciso 2° del artículo 14.

ii. Recibir las solicitudes de rectificación y cancelación efectuadas por el titular, previa autenticación de éste, y luego remitirlas al administrador del registro, en conformidad al inciso 2° del artículo 14.

¹¹⁷ De acuerdo al artículo 2 letra g) serán las sociedades que cumpliendo con las disposiciones de la presente ley, de los reglamentos que de ella emanen y de la normativa dictada por la autoridad competente, en forma habitual recolectan, almacenan, sistematizan, modelan, comercializan, publican, difunden y, en general, realizan tratamiento de datos de obligaciones económicas y de otros datos, de personas naturales y jurídicas, y que además elaboran productos de valor agregado y prestan servicios relacionados con la información tratada.

iii. Recibir y entregar, con los debidos resguardos de confidencialidad, el Reporte Anual y cualquier otra información que el registro remita al Titular.

iii. Informar al público y mantener actualizada dicha información respecto de las siguientes materias:

- La forma de obtención del reporte anual.
- Los derechos contemplados en la presente ley y en la Ley N° 19.628, y los procedimientos a seguir en cada caso.
- Significado de las siglas, símbolos y abreviaturas que se utilicen en los Informes Comerciales.

iv. Elaborar y mantener, un registro con la información relativa a tramitación de reportes anuales; solicitudes de rectificación y de cancelación, y de reclamos de Titulares, de acuerdo a las normas establecidas por la Superintendencia de Bancos e Instituciones Financieras para ello.

v. Llevar un registro de los usuarios que han consultado la información del titular en los últimos doce meses.

vi. Informar al titular, previo pago de una tarifa, de un listado de los usuarios que hayan requerido su Informe durante los últimos doce meses.

4. Derecho a ser informado manifestado como derecho de rectificación y cancelación.

Lo que vendría siendo el artículo 15 del Proyecto de Ley sobre deuda positiva y negativa de los chilenos establece que:

i) El titular tendrá derecho a impugnar los datos contenidos en el Registro Central de Obligaciones Económicas.

La solicitud deberá tener las siguientes características:

- Deberá ser presentada por escrito solicitando la rectificación o cancelación de los datos.
- Deberá indicar las razones o antecedentes de su petición, adjuntando copia del reporte o informe que le da origen, además del documento donde consta que el dato es erróneo, caduco, inexacto o incompleto respecto del mismo, o una declaración jurada simple de ser la obligación a que se refiere el dato impugnado, inexistente.

ii) El titular podrá concurrir ante el aportante responsable del dato cuestionado o ante una distribuidora u otro canal que determine la Superintendencia de Bancos e Instituciones Financieras, dentro de un plazo de 15 días desde que ha tomado conocimiento de que el dato a que se refiere es erróneo, caduco, inexacto o incompleto.

a. Si concurre ante el aportante: el aportante deberá comunicar al administrador del Registro Central de Obligaciones Económicas que ha recibido una solicitud de rectificación o cancelación. El aportante deberá resolver la solicitud sea entregando la información corregida o negándose a ello y comunicar la respuesta al afectado y al administrador del registro, dentro del plazo de 15 días.

b. Si concurre ante una distribuidora u otro canal que determine la Superintendencia: la entidad deberá remitir, la respuesta al afectado, al administrador del Registro Central de Obligaciones Económicas dentro de un plazo de 15 días. El administrador estará obligado a remitir al aportante las solicitudes de rectificación o cancelación que haya recibido.

iii) Cuando el administrador del Registro Central de Obligaciones Económicas haya recibido la solicitud de reclamo del titular, deberá incluir la leyenda “registro impugnado” en el historial del titular y una indicación del tipo de reclamo, la que se deberá mantener mientras dure el procedimiento de rectificación o cancelación.

iv) Si la impugnación consiste en la inexistencia de la obligación, el aportante tendrá un plazo de 48 horas para acreditar su existencia. De no acreditarse la existencia de la obligación, el dato quedará bloqueado en los términos del artículo 2º, letra b), de la Ley N°19.628.

v) En la eventualidad de que la respuesta del aportante no sea satisfactoria, el afectado podrá recurrir dentro del plazo de quince días, contado desde la notificación de la respuesta, al Consejo para la Transparencia y Protección de Datos Personales, ajustándose al procedimiento que contempla la misma indicación sustitutiva, procediendo recurso de ilegalidad ante la Corte de Apelaciones.

El proyecto señala en su artículo 17 que los procedimientos y plazos para ejercitar el derecho de información, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente, de manera que se remite a otro cuerpo normativo que detalle acabadamente el ejercicio del derecho a ser informado.

Así, por ejemplo, el contenido del reporte anual, los procedimientos y plazos de su solicitud y entrega serían regulados por este reglamento.

Incumplimiento de la obligación de informar al titular de los datos en sus distintas modalidades.

Las labores de supervisión y fiscalización, respecto al cumplimiento de las disposiciones legales y reglamentarias relativas a las entidades que participan en el tratamiento de información comercial, estarán a cargo de la Superintendencia de Bancos e Instituciones Financieras, a la que le corresponderá supervisar y fiscalizar a las entidades correspondientes, cerciorándose del debido cumplimiento de las obligaciones que establece el proyecto.

Ya señalamos que si el titular de los datos quiere impugnar los datos contenidos en el registro podrá solicitar por escrito su rectificación y cancelación al aportante responsable, a la distribuidora u otro canal que determine la Superintendencia y, en el caso que no quede conforme, podrá recurrir ante el Consejo para la Transparencia y

Protección de Datos Personales. Es importante subrayar que estos recursos no se conceden para los casos en que se infrinja el derecho de acceso.

Además, de acuerdo al artículo 23, los afectados como consecuencia del incumplimiento tendrán derecho a ser indemnizados por las entidades fiscalizadas responsables del tratamiento de datos. Se presume legalmente la responsabilidad del autor del daño, si existe infracción a la ley.

Simultáneamente a estas instancias, el Proyecto de Ley establece una serie de infracciones que pueden tener el carácter de leves, graves y gravísimas, sin perjuicio de las sanciones penales establecidas en la ley N° 19.233¹¹⁸ que realmente no tipifican conductas de infracción al derecho a ser informado.

Las nuevas disposiciones sancionan tangencialmente la infracción al derecho a ser informado, estableciéndose vagamente que se considera:

i. Infracción leve:

- No cumplir con la obligación de informar de acuerdo a lo señalado en el artículo e) y h).

¹¹⁸ La ley N° 19.233 se compone de los siguientes cuatro artículos:

“Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”.

- Los tratos y cobros indebidos o discriminatorios por parte de las distribuidoras a los titulares y usuarios.
- Los tratos y cobros indebidos o discriminatorios de las obligaciones impuestas por esta ley y por parte de los aportantes a los titulares y usuarios.
- No informar al Registro Central de Obligaciones Económicas de las solicitudes de impugnación o rectificación.

ii. Infracción grave:

- No dar cumplimiento a las instrucciones de la Superintendencia de Bancos e Instituciones Financieras para la validación, actualización periódica y rectificación de la información.
- La no incorporación, por parte el administrador del Registro Central de Obligaciones Económicas, de la leyenda "Registro Impugnado", de conformidad al artículo 15.
- La reiteración de infracciones leves, es decir, cuando se cometan dos o más infracciones de este carácter, en un período no superior a 6 meses.

iii. Infracción gravísima.

- La reiteración de infracciones graves, es decir, cuando se cometan dos o más infracciones de este carácter, en un período no superior a 6 meses.

Como vemos, el proyecto no establece sanciones estrictamente directas al incumplimiento del deber de información, sino sólo sanciones generales por infracción

a los principios que subyacen la legislación de protección a la información económica¹¹⁹.

La modificación sustitutiva establece montos pecuniarios frente a las infracciones de privados, fluctuando en los siguientes valores:

- Para infracciones leves cometidas por privados: multas de hasta 200 UTM¹²⁰, es decir, hasta alrededor de \$7.350.400.
- Para infracciones graves cometidas por privados: multas de hasta 5.000 UTM, es decir, hasta alrededor de \$180.760.000.
- Para infracciones gravísimas cometidas por privados: multas de hasta 10.000 UTM, es decir, hasta alrededor de \$367.520.000.

En este contexto, resulta sorprendente que el Proyecto de Ley se anuncie como una medida acorde a la protección de los datos personales de las personas, señalando la Subsecretaria de Hacienda, María Olivia Recart, al presentar la modificación sustitutiva:

“Nuestro foco es que cada persona decida qué datos, sobre deuda al día quiere usar... A veces la gente no tiene cómo demostrar ingresos, pero sí puede demostrar que paga sus deudas¹²¹”.

¹¹⁹ Cabe señalar que el catálogo de infracciones es mucho más amplio y sólo se incluyeron las que regulaban tangencialmente el derecho a ser informado del tratamiento de datos personales.

¹²⁰ UTM calculada de acuerdo al mes de marzo de 2010.

¹²¹ Cooperativa.cl, tópicos economía, nacional, endeudamiento, Proyectos de ley sobre datos personales protegen al consumidor, destacó Hacienda [En línea], Santiago, 12 de mayo de 2009, http://www.cooperativa.cl/proyectos-de-ley-sobre-datos-personales-protegen-al-consumidor--destaco-hacienda/prontus_notas/2009-05-12/073335.html [Consulta 10 de julio de 2009]

La opinión de Peter Hill, Presidente de la Cámara de Comercio de Santiago es categórica:

"Para mí es un error que el Proyecto de Ley vaya hoy al Parlamento, porque en este momento está en trámite en la Cámara de Diputados el Proyecto de Ley sobre datos personales, que apunta hacia (una mayor) privacidad de las personas. Obviamente que esto otro va en sentido contrario, va a ir en contra también del empleo. Seamos claros, mientras más información se tenga de las personas va a ser más difícil para ellas conseguir trabajo. En Chile llevamos siete u ocho meses de crisis y el endeudamiento y la morosidad efectivamente han aumentado, pero en forma leve, y el país sigue consumiendo. Preocúpense hoy de hacer medidas pro empleo, de ayudar a la gente, en vez de atacar algo que ha funcionado y que ha dado buenos resultados. El comercio le ha dado crédito a millones de personas en este país, para que mejore su calidad de vida. Y hoy, como están funcionando las cosas, cada persona que solicita un crédito puede ir a la casa comercial donde se le va a entregar un certificado que diga exactamente si está moroso o no. Entonces, ¿de qué me están hablando, para qué se necesita (la ley)?"¹²².

Lo que parece más alarmante es que se promueva esta modificación sustitutiva como un proyecto que incita a la protección de los datos personales de categoría económica y a la autodeterminación informativa de los individuos, en el sentido que podrían elegir cómo utilizar sus datos económicos positivos, cuando el texto de la ley señala todo lo contrario, promueve una gran cantidad de recolección de datos, de distintas fuentes y de diferentes actores del mercado, sin fortalecer el derecho de los individuos a optar

¹²² Peter Hill: "No estamos de acuerdo con que la base de datos (...) vaya a dar a un ente estatal", Entrevista, El Mercurio, martes 12 de mayo de 2009.

por qué información está siendo tratada y sin dotarlos de un óptimo derecho de información al momento de tratar los datos personales.

Incluso, en la hipótesis más optimista, si nos planteáramos la posibilidad de educar a los consumidores, poniéndolos en conocimiento del funcionamiento del mercado crediticio y el sistema de información comercial, podríamos pensar en el ideal de un uso responsable de los derechos de acceso frente al Registro Central de Obligaciones Económicas, sin embargo, sólo se podrá acceder a estos gratuitamente una vez al año y el resto de las veces tendría que pagar una tarifa.

CONCLUSIONES FINALES.
EL DERECHO A SER INFORMADO COMO SUSTENTO FUNDAMENTAL
DEL CONTROL DE DATOS PERSONALES.

La tecnología actual posibilita una capacidad de tratamiento y transmisión de información sin precedentes, consecuencia del desarrollo de los computadores y su implementación en todas las áreas de la sociedad. Mega-archivos, data warehouse y datavigilancia son herramientas de uso masivo que han traído consigo una intensa modificación en cuanto a la conceptualización, almacenamiento y procesamiento de los datos personales de los individuos.

El proceso de informatización no tiene marcha atrás. La acumulación de información personal, lejos de detenerse, evidencia una evolución constante que tras los beneficios que conlleva, disimula los perjuicios latentes que podrán recaer en los individuos titulares de la información recolectada. En efecto, podemos reconocer la importancia de una íntegra, exacta y correctamente empleada información, pero este reconocimiento no puede implicar la inmolación de la persona en aras del acopio de información.

Los datos de las personas no constituyen informaciones aisladas, por el contrario, pueden llegar a revelar facetas sustanciales de los individuos, cristalizándolos en una serie de afirmaciones sobre lo que la persona es, lo que piensa o como actúa. De aquí que surja la necesidad de preservarla frente a la potencial agresividad de la acumulación de cantidades impensadas de datos personales, estableciendo un equilibrio entre los actores de esta relación que el derecho debe someter a determinadas disposiciones normativas para evitar el abuso de la tecnología, en detrimento de la protección de las personas.

Dada la cantidad de bienes, los derechos individuales y colectivos implicados y su calificación jurídica, la protección de datos personales no es un tema alejado de la

controversia. Los elementos en juego son de diversa índole, apuntan a la ideología, al pensamiento, a la libertad, a la intimidad y a otros cuantos derechos asociados. De aquí que pretender regular la protección de los datos personales, únicamente en función de la intimidad es una concepción altamente insuficiente, ya que este derecho debe cautelarse con una entidad propia y diferenciada.

Descifrar su significado, determinar su estructura y definir sus limitaciones ha ocasionado el debate propio de derechos que están comenzando a gestarse y asentarse. La finalidad de los cuerpos legislativos que hagan eco de esta discusión siempre será similar, y consiste en decidir acerca del calificativo de derecho y la modalidad de reconocimiento de la protección de los datos personales.

La respuesta que el derecho ha dado a estas interrogantes dista de ser uniforme, por el contrario, ha seguido distintos caminos, no coincidentes en cuanto a su origen pero sí en cuanto a su contenido y significado, al menos en una valoración final de su conjunto¹²³.

La protección de los datos personales fue concebida en sus comienzos como un derecho contenido y consecuencia de la protección a la intimidad. Sin embargo, progresivamente las legislaciones nacionales han aceptado que para otorgar una adecuada protección al espacio de la libertad de las personas, fuertemente asociada a la intimidad, es necesario dotarse de un concepto más amplio que permita proteger el conjunto de derechos del individuo que pueden ser vulnerados en el tratamiento de datos personales.

Esa afirmación no ignora el papel que ha desempeñado la intimidad en la construcción de un derecho a proteger los datos personales, pero sí intenta rechazar su identificación total con ella pues ambas no recaen en la misma realidad jurídica, la que se ha desarrollado bajo presupuestos diametralmente distintos.

¹²³ SERRANO Pérez, María Mercedes, El derecho fundamental a la protección de datos. Derecho español y comparado, Madrid, Thompson, Civitas, 2003, Pág. 482.

De esta forma el derecho a la protección de datos reivindica un contenido distinto al de la intimidad y de cualquier otro derecho fundamental. Éste es en sí mismo un auténtico derecho que supera los límites de la intimidad pero que afecta otros cuantos derechos fundamentales.

Precisamente esta misma concepción ha sido desarrollada por los textos internacionales, especialmente el Convenio 108 del Consejo de Europa de 1981 y más recientemente la Directiva 95/46 del año 1995. La conformación de leyes de protección de datos bajo el prisma de estos cuerpos normativos, deviene en la proclamación de un derecho de protección de datos que se traduce en un derecho del titular de los datos a controlar la información que le concierne sobre su propia persona.

Este derecho a controlar los datos personales, perfila un auténtico derecho fundamental a la protección de datos, tal como lo percibieron el Tribunal Federal Alemán, cuando resolvió el recurso interpuesto contra la Ley de Censo de la Población; y, el Tribunal Constitucional de España a través de la sentencia 254/1993 que profundiza sobre el alcance del artículo 18.4 de la Constitución. Ambos tribunales conceptualizaron un nuevo derecho denominado autodeterminación informativa y libertad informática, correspondientemente, cuyo contenido se centra, específicamente, en el derecho del titular de los datos a controlar su información personal, determinando quién, cómo, cuándo y por qué conoce sus datos y ejerciendo las facultades necesarias para cautelar el ejercicio de este derecho.

Esta visión ha sido progresivamente incorporada a las diferentes legislaciones de los países, sin embargo, resulta curiosa la gran disparidad entre éstas, pese a que internacionalmente se cuenta con directrices valiosísimas que aportan un claro modelo según el cual debe estructurarse un sistema ideal de protección de datos personales.

La protección de datos adecuada ha avanzado hacia un sistema eficiente que establece obligaciones específicas para los responsables del tratamiento de datos y derechos correlativos para los titulares de la información. El derecho a controlar los

datos personales, que se ha plasmado en las leyes más avanzadas en esta materia, contiene como base y fundamento estos derechos para el titular del banco de datos. Asimismo, el ejercicio de este entramado de facultades se condiciona intrínsecamente a los derechos de información que se consagran a favor del individuo, los que permitirán ejercer, consecuentemente, los derechos a consentir en el tratamiento de los datos personales, a acceder a éstos y a solicitar su modificación, eliminación y bloqueo.

Un sistema que no provea un derecho a ser informado de una calidad adecuada, estará destinado al fracaso, precisamente por la misma naturaleza que subyace al tratamiento, la que más allá de tener un carácter altamente silencioso y disimulado, encubre sus riesgos tras los beneficios que reportan actividades de este tipo, altamente productivas desde un punto de vista estratégico y económico.

Para la estructuración de un adecuado derecho de protección de datos personales materializado en un derecho a controlar la información que le concierne al propio individuo, el sistema legal del país debe ser permeable al reconocimiento de estas facultades asociadas. En efecto, en la mejor hipótesis se le otorgará el máximo rango legal a estas facultades, a los derechos a conocer, acceder, modificar, eliminar o bloquear los datos personales cuando corresponda. Sin embargo, entendiendo que estamos ante un derecho en construcción, relativamente nuevo, el hecho de que determinado país no consagre de manera expresa un derecho fundamental específico a controlar los datos personales, no quiere decir, que lo despoje de reconocimiento alguno, sino que efectivamente puede reconocerlo de forma tangencial.

Al preguntarnos sobre la situación de nuestro país, si lo comparamos con otras experiencias nacionales, nuestro sistema jurídico no contiene ningún precepto de rango constitucional que consagre el derecho a controlar los datos personales. El reconocimiento de estas facultades asociadas se ha realizado a través de la ampliación del concepto de vida privada consagrado en el artículo 19 N° 4 que permitiría el establecimiento de estas facultades tan esenciales. Así lo podemos observar en el siguiente cuadro:

PAÍS	RECONOCIMIENTO CONSTITUCIONAL DEL DERECHO A CONTROLAR LOS DATOS PERSONALES
CHILE	Extensión del Art. 19 N° 4: La Constitución asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y su familia.
ESPAÑA	Art. 18.4: La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos.
ARGENTINA	Art. 43: Toda persona podrá interponer esta acción (de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.
COLOMBIA	Art. 15: Se reconoce a las personas el derecho a conocer, actualizar y rectificar las informaciones que hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas o privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
MÉXICO	<p>Art. 6: Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas consecuencias, se regirán por los siguientes principios y bases: II. La información a que se refiere la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.</p> <p>Art. 16 inc. 2: Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.</p>

El reconocimiento de un derecho de control de datos personales de rango constitucional no se traduce en una mejor calidad de protección. La ley general que consagra y desarrolla este derecho es igual o, incluso, más relevante. Por ejemplo, México cuenta con un completísimo derecho a controlar los datos personales de rango constitucional pero no posee una ley capaz de otorgar una íntegra protección.

Lo relevante es entonces que el sistema jurídico permita el reconocimiento incuestionable del derecho a controlar la información personal informatizada, garantizando con ello la libertad del individuo, una libertad de tipo inmaterial que

trasciende todos los derechos de la persona. Este ámbito de libertad individual frente a la informática, se concede otorgando a la persona una capacidad de decisión y control sobre sus informaciones personales, facultades que pueden consagrarse constitucional o legalmente. No negaremos que lo más óptimo sería una proclamación como la del artículo 15 o del artículo 16 inciso 2 de Colombia y Argentina, respectivamente, que no dejan espacio a discusiones de tipo doctrinario sobre el reconocimiento del derecho y su extensión. Sin embargo, como ya señalamos, las disposiciones constitucionales no lo son todo, y deben proveerse de leyes que desarrollen los preceptos cuando esto sea necesario, otorgando facultades concordantes con las consagradas en el texto constitucional que aseguren el cumplimiento de las disposiciones.

En efecto, no solucionaríamos los problemas que trascienden a nuestra Ley N° 19.628 de Protección a la Vida Privada, si antes de dictarla, el legislador hubiera encuadrado entre los derechos fundamentales, un derecho expreso a controlar los datos personales. La ley aún no permitiría el cumplimiento irrestricto de las obligaciones consagradas para los responsables de los bancos de datos, ni tampoco respecto a los derechos dispuestos para los titulares de los datos.

Observemos ahora, como desarrollan, las leyes generales, el derecho a controlar los datos personales a través del derecho que se le concede al titular de los datos personales a ser informado en sus distintas manifestaciones, contrastándolos a través de cuadros comparativos, con las directrices internacionales consagradas y los derechos de información que disponen nuestra Ley N° 19.628 de Protección a la Vida Privada y los Proyectos de Ley que pretenden introducir modificaciones, estableciendo las opciones más eficaces para la protección de los datos personales.

Analizaremos:

1. El derecho a ser informado en caso de obtención de datos recabados del propio titular.

2. El Derecho a ser informado en caso de obtención de datos recabados de un tercero.
3. El Derecho a ser informado manifestado como derecho de acceso.
4. El Derecho a ser informado manifestado como derecho de rectificación, supresión y bloqueo.
5. El Derecho a ser informado manifestado como derecho de consulta ante la autoridad de control.
6. Incumplimiento al derecho a ser informado en sus distintas manifestaciones.

1. El Derecho a ser informado en caso de obtención de datos recabados del propio titular.

PAÍS	DERECHO A SER INFORMADO EN CASO DE OBTENCIÓN DE DATOS DEL PROPIO TITULAR DE LOS DATOS PERSONALES
CHILE Ley N° 19.628	<p>El artículo 3 únicamente contempla un derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública. Se debe informar al titular:</p> <ol style="list-style-type: none"> i. El carácter obligatorio y facultativo de las respuestas. ii. El propósito para el cual se está solicitando la información.
CHILE Proyecto de Ley 687-356	<p>Al artículo 3 que contempla el derecho a ser informado en actividades de encuesta, sondeo, mercadeo y opinión pública se complementa, disponiéndose que debe informarse sobre:</p> <ol style="list-style-type: none"> i. El carácter obligatorio y facultativo de las respuestas. ii. El propósito para el cual se está solicitando la información. iii. Las consecuencias jurídicas de la negativa a responder las preguntas realizadas. iv. La finalidad para la cual se está solicitando la información. v. Los destinatarios de los datos. vi. La posibilidad de que estos datos sean comunicados a terceros. <p>Además se agrega un Art. 3 bis que dispone que deberá informarse de modo expreso, preciso, claro e inequívoco en toda solicitud de datos sobre:</p> <ol style="list-style-type: none"> i. La existencia de un registro o banco de datos personales en el cual se consignará la información, identidad del titular del banco de datos y su domicilio, la finalidad de la recogida de datos y los destinatarios de la información. ii. El carácter obligatorio o facultativo de la entrega de datos personales que se le soliciten y las consecuencias de la entrega de los datos o de la negativa a suministrarlos. iii. Los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo. iv. El derecho a revocar su autorización para el tratamiento de datos que le conciernen y las consecuencias de su revocación. v. Una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten. vi. De la circunstancia de que los datos proporcionados vayan a formar parte de un registro o banco de datos de acceso público.

CHILE Proyecto de Ley sobre deuda positiva y negativa de los chilenos	No se consagra el derecho de información en la solicitud de datos del propio titular.
ESPAÑA Ley Orgánica 15/1999	El artículo 5 N°1 de la Ley Orgánica española dispone que cuando la información se recabe del propio titular se deberá informar de forma expresa, precisa e inequívoca sobre los siguientes aspectos: i. La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. ii. El carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. iii. Las consecuencias de la obtención de los datos o de la negativa a suministrarlos. iv. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. v. La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
ARGENTINA Ley N° 25.326	El artículo. 6 señala que cuando se requieran datos debe informársele, en el acto, de forma expresa y clara acerca de: i. La finalidad para la que serán tratados los datos y quienes pueden ser sus destinatarios o clase de destinatarios. ii. La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. iii. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles. iv. Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. v. La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de datos.
COLOMBIA Ley Estatutaria 1.266	El artículo 4 letra b señala que la fuente de información debe informar al titular de los datos, únicamente, sobre la finalidad de la recogida de datos, previa o concomitantemente, con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto.
MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	El artículo 20 apartado III señala que los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61.

El modelo rector para el establecimiento de este derecho es el otorgado por la Directiva 95/46 que establece que los Estados deben disponer que el responsable del tratamiento comunique al titular de los datos, por lo menos la identidad del responsable del tratamiento y los fines que trascienden al tratamiento de los datos. El punto más importante a destacar aquí es que el hecho que los datos sean recogidos del propio titular implica un posible conocimiento de éste respecto a los puntos a

informar, de aquí que la Directiva advierte que en estos casos no es necesario otorgar dichas informaciones.

Llama la atención que este sea uno de los derechos de información más desarrollados en las leyes generales de protección de datos personales como si fuera el más relevante, cuando en la práctica lo que sucede es lo contrario. Por ejemplo, de aceptarse la modificación a la Ley N° 19.628 se establecería este derecho en dos artículos que tienen el mismo objetivo. Es decir, resultaría redundante la hipótesis del artículo 3 y el artículo 3 bis, cuando lo más óptimo sería dejar solo el artículo 3 bis porque incluye al artículo 3 en extensión y tiene una redacción más adecuada. Como decíamos, cuando los datos se recogen del propio titular, existirá una conciencia de éste acerca de estar otorgando a un tercero sus datos personales y en este sentido se encuentra en una posición bastante cómoda como para negarse a entregar sus datos, en caso de desconfianza, o bien, derechamente preguntar sobre la identidad del responsable del tratamiento y la finalidad de la recogida de datos, lo que se podrá realizar en el mismo acto de la recolección, de manera que la importancia de establecer un plazo para la información decae.

2. Derecho a ser informado en caso de obtención de datos recabados de un tercero.

PAÍS	DERECHO A SER INFORMADO EN CASO DE OBTENCIÓN DE DATOS DE TERCEROS
CHILE Ley N° 19.628	Esta hipótesis no se contempla expresamente. Sólo se trata tangencialmente respecto al deber de informar al requerir autorización para el tratamiento de datos personales en el artículo 4 (Regla general será no requerir el consentimiento del afectado).
CHILE Proyecto de Ley 687-356	El artículo 3 bis señala que deberá informarse al titular de los datos de forma expresa, precisa, clara e inequívoca, dentro de los tres meses siguientes al momento de recogida de los datos objeto de tratamiento: i. Los datos objeto de tratamiento. ii. La procedencia de los datos. iii. La existencia de un registro o banco de datos personales en el cual se consignará la información, identidad del titular del banco de datos y su domicilio, la finalidad de la recogida de datos y los destinatarios de la información. iv. Los derechos que le asisten en virtud de la ley, especialmente el derecho de acceso, rectificación, cancelación y bloqueo. v. El derecho a revocar su autorización para el tratamiento de datos que le conciernen y las

	<p>consecuencias de su revocación.</p> <p>vi. Una dirección física o electrónica válida en la cual pueda ejercer los derechos que le asisten.</p>
<p>CHILE Proyecto de Ley sobre deuda positiva y negativa de los chilenos</p>	<p>De acuerdo al artículo 13 se establece que los aportantes deberán informar al titular , cuando éste lo solicite por escrito, sobre:</p> <p>i. La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen.</p> <p>ii. El contenido de la información, que incluye entre otros, la individualización del titular y del aportante, los montos de las obligaciones económicas a que se refieren y la fecha en que se contrajo la obligación.</p> <p>iii. El propósito del tratamiento de los datos.</p> <p>iv. Los destinatarios y cesionarios de los datos, distintos del registro, de los últimos doce meses.</p> <p>v. Si su historial ha sido utilizado para tomar una decisión adversa o favorable.</p> <p>vi. De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.</p>
<p>ESPAÑA Ley Orgánica 15/1999</p>	<p>El artículo 5 N° 4 señala que el responsable del fichero o su representante deberán informar dentro del plazo de tres meses, siguientes al momento del registro, salvo que ya hubiera sido informado con anterioridad:</p> <p>i. Del contenido del tratamiento.</p> <p>ii. De la procedencia de los datos.</p> <p>iii. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.</p> <p>iv. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.</p> <p>v. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.</p>
<p>ARGENTINA Ley 15.326</p>	<p>No se establece este derecho en específico, sólo se hace una referencia general al “momento de recabar datos personales” del artículo 6.</p>
<p>COLOMBIA Ley Estatutaria 1.266</p>	<p>Este derecho no se contempla para la generalidad de los datos. No existe este deber para la fuente, los operadores, ni tampoco los usuarios. Este deber se establece sólo respecto de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. En estos casos la fuente de información debe informar al titular de los datos previamente a la remisión del reporte como lo establece el artículo 12 inciso 2 y 3, deber que podrá cumplirse a través de los extractos periódicos enviados al domicilio del cliente.</p>
<p>MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental</p>	<p>No se consagra este derecho.</p>

Pareciera que ha sido difícil distinguir para los legisladores de los distintos países, que la recogida de datos personales no se realiza siempre desde el mismo titular de los datos, sino que por el contrario, la gran mayoría de las veces los datos son recabados desde una tercera persona u órgano que transmite la información que maneja. Precisamente, esta modalidad de tratamiento es la que el derecho de protección de datos personales debe proteger con mayor énfasis, estableciendo disposiciones claras que diferencien la fuente de la que trasciende la información y cómo el responsable del nuevo fichero debe cumplir con el deber de informar sobre este tratamiento.

La información que otorgue el nuevo responsable del fichero debe ser mucho más amplia que la otorgada para la hipótesis de recogida desde el mismo titular, pues debemos partir de la suposición que el afectado desconoce absolutamente el tratamiento que se está efectuando de sus datos, y precisamente por esta misma razón, en aquel tratamiento residen potenciales daños de mayor magnitud.

El Convenio 108 del Consejo de Europa no efectuó distinción entre quién era el sujeto del que se recababan los datos personales. Sólo con la Directiva 95/46 esta diferenciación se hizo nítidamente, estableciéndose que los Estados miembros deberían disponer que el responsable del tratamiento o su representante informen, desde el momento del registro de los datos o, a más tardar, en el momento de la primera comunicación de datos, en caso que se piense comunicar datos a un tercero, por lo menos la identidad del responsable del tratamiento, los fines de éste y cualquier otra información.

El desarrollo de este derecho debería avanzar hacia su reconocimiento expreso, el establecimiento de plazos concretos para evacuar la información, aunque sea en la modalidad de una notificación, siempre realizada de oficio, es decir, sin necesidad de que sea el titular quien deba instar a su cumplimiento, más aún cuando difícilmente se puede obstar al ejercicio de un derecho sobre el cual su vulneración se desconoce. Por último, la información debiera extenderse a la existencia del fichero donde constan datos del afectado, la individualización del responsable del fichero, las finalidades que trascienden al tratamiento y la existencia de derechos de acceso, modificación, bloqueo y eliminación cuando corresponda.

3. Derecho a ser informado manifestado como derecho de acceso.

PAÍS	DERECHO A SER INFORMADO MANIFESTADO COMO DERECHO DE ACCESO
CHILE	El artículo 12 señala que toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales:

Ley N° 19.628	<ul style="list-style-type: none"> i. Información sobre los datos relativos a su persona. ii. La procedencia de los datos. iii. El destinatario de los datos. iv. EL propósito de almacenamiento. v. La individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.
CHILE Proyecto de Ley 687-356	Se conserva el artículo 12 en su integridad y se agrega un nuevo punto a informar que consiste en "las evaluaciones y apreciaciones que sobre dicha información hayan sido comunicadas durante los últimos seis meses, así como los criterios de apreciación empleados, el nombre y dirección de la persona o entidad a quien haya comunicado los datos".
CHILE Proyecto de Ley sobre deuda positiva y negativa de los chilenos	<p>El artículo 14 señala que todo titular tiene derecho a acceder, en las condiciones establecidas en la ley y sus reglamentos, a sus datos de obligaciones económicas que son objeto de tratamiento por parte de las entidades fiscalizadas.</p> <ul style="list-style-type: none"> - El titular puede solicitar y recibir gratuitamente de administrador del Registro Central de Obligaciones Económicas un reporte anual que contendrá: <ul style="list-style-type: none"> i. La identificación de los acreedores del titular. ii. Todo otro tipo de información relativa a los acreedores del titular que se encuentre disponible en el Registro Central de Obligaciones Económicas. - El titular tendrá derecho a tomar conocimiento, gratuitamente y en cualquier época, únicamente de la identidad de sus acreedores incluidos en el Registro Central de Obligaciones Económicas. - Previo pago de una tarifa permanente el titular podrá ser informado de: <ul style="list-style-type: none"> i. Los datos que sobre él existen en el registro. ii. Los informes comerciales de las distribuidoras. iii. Quiénes han recibido dicha información en los últimos doce meses.
ESPAÑA Ley Orgánica 15/1999	<p>El artículo 15 dispone que el titular de los datos tendrá derecho a solicitar y obtener gratuitamente, a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo al efecto, la siguiente información:</p> <ul style="list-style-type: none"> i. Los datos carácter personal sometidos a tratamiento. ii. El origen de sus datos sometidos a tratamiento. iii. Las comunicaciones realizadas o que se prevén hacer de los datos sometidos a tratamiento.
ARGENTINA Ley 25.326	El artículo 14 contempla el derecho de acceso que podrá ejercerse gratuitamente y a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. El titular, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. Frente a la solicitud, el responsable de datos tiene diez días corridos, si no se satisface la solicitud o si el informe se estima insuficiente procede acción de hábeas data.
COLOMBIA Ley Estatutaria 1.266	Según el artículo 6.1.1 el derecho a acceder a los datos se ejerce frente a los operadores de los bancos de datos. El derecho acceso también puede ejercerse frente a la fuente, pero ésta deberá ser reenviada al operador, pues será éste quien dé cumplimiento al derecho.
MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	El artículo 24 de la ley dispone que el titular de los datos tiene derecho a acceder a sus datos personales, solicitando a una unidad o enlace o su equivalente, previa acreditación, que le proporcione los datos personales que obren en un sistema de datos personales.

El derecho de acceso es una de las facultades más emblemáticas del derecho a ser informado y que en sus consagraciones más formales, se ha acogido en la legislación

nacional a un nivel constitucional específico como una acción de hábeas data derivada de la acción de amparo que se refiere a la facultad del individuo a exigir que se muestre o exhiba el dato.

El derecho de acceso se desarrolla en un nivel temporal distintos que los derechos analizados en el punto 1 y 2, ya que este derecho se ejerce cuando el individuo ha adquirido cierto grado de certeza respecto a la existencia del banco de datos y desea conocer específicamente su contenido, es decir, los datos que se encuentran enlistados en el registro.

El derecho de acceso fue consagrado en el Convenio 108 del Consejo Europea, el que dispuso que el titular tiene derecho a obtener, a intervalos razonables y sin demora o gastos excesivos, la confirmación de la existencia o inexistencia del fichero de datos personales que conciernan a la persona y la comunicación de dichos datos en forma inteligible. Luego, la Directiva 95/46 señala que los Estado miembros deben garantizar a los interesados el derecho a que se les comunique:

- i. La confirmación de la existencia o inexistencia del tratamiento de datos personales.
- ii. Los fines del tratamiento.
- iii. Las categorías de datos a que se refiere el tratamiento.
- iv. Los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos.
- v. Los datos objeto de tratamiento.
- vi. La lógica utilizada en los tratamientos automatizados de datos.

El derecho de acceso, en la mayoría de las legislaciones, y en el caso chileno propiamente tal, no es un derecho que contenga falencias en su teoría, es decir, el derecho está planteado en una forma muy íntegra y completa, estableciéndose los plazos a los que está sujeto y una completa descripción de lo que debe ser informado por el responsable del banco de datos.

Los problemas de este derecho se presentan en la práctica por debilidades en otras etapas del sistema y que dicen relación con el desarrollo de los recursos, la fiscalización del órgano de control y el grado de exactitud del registro que lleve este órgano fiscalizador. Nuestra legislación actual contiene todas estas falencias. En efecto, el recurso de reclamación concedido es inadecuado porque no permite la celeridad requerida del proceso y su ejercicio puede llevar a acarrear costos demasiado altos para la mayoría de los titulares. Además no se establece un órgano de control y se dispone la existencia de un catastro nacional de bases de datos únicamente para los ficheros de titularidad pública.

La buena noticia es que todas estas debilidades han sido captadas por el proyecto y enmendadas, de forma que el derecho de acceso debería tener un mejor pronóstico de acogerse las modificaciones que plantea la moción. El único punto criticable es respecto la modificación sustitutiva sobre deuda negativa y positiva de los chilenos que no establece un real derecho de acceso gratuito pues este se consagra sólo en apariencia ya que para conocer el real contenido de los datos que constan en el fichero, el titular tendrá que pagar una suma de dinero siempre. El acceso gratuito que se puede ejercer una vez al año sólo contendrá la identificación de los acreedores del titular y todo otro tipo de información relativa a éstos que se encuentre disponible en el Registro Central de Obligaciones Económicas.

4. Derecho a ser informado manifestado como derecho de consulta ante la autoridad de control.

PAÍS	DERECHO A SER INFORMADO MANIFESTADO COMO DERECHO DE CONSULTA ANTE LA AUTORIDAD DE CONTROL
CHILE Ley N° 19.628	De acuerdo al artículo 22 el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo solamente de organismos públicos. Este registro tendrá carácter público y en él constará: i. El fundamento jurídico de la existencia del banco de datos. ii. Su finalidad. iii. Los tipos de datos almacenados y la descripción del universo de personas que comprende. El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde

	<p>que se produzca. No existe sistema de registro para los bancos de datos privados.</p>
<p>CHILE Proyecto de Ley 687-356</p>	<p>Se agrega al artículo 12 un nuevo inciso primero que señala que toda persona podrá solicitar al Registro Único Nacional de Bancos de Datos, de carácter público y gratuito, información sobre:</p> <ul style="list-style-type: none"> i. La existencia del tratamiento de datos de carácter personal que pudieren afectarle. ii. Las finalidades del tratamiento de datos. iii. Todos los antecedentes necesarios para la identificación del responsable del tratamiento. <p>Este registro será mantenido por el Consejo para la Transparencia y la Protección de Datos Personales, como órgano de control.</p>
<p>CHILE Proyecto de Ley sobre deuda positiva y negativa de los chilenos</p>	<p>No existe. Este derecho no se contempla frente al Consejo para la Transparencia y la Protección de Datos Personales, ni tampoco frente a la Superintendencia de Bancos e Instituciones Financieras que ejerce labores de supervisión y control frente a las entidades que participan en el tratamiento de la información comercial.</p>
<p>ESPAÑA Ley Orgánica 15/1999</p>	<p>De acuerdo al artículo 14, cualquier persona podrá conocer, recabando la información oportuna del Registro General de Protección de Datos Personales, de consulta pública y gratuita:</p> <ul style="list-style-type: none"> i. La existencia del tratamiento de datos de carácter personal. ii. Las finalidades del tratamiento de datos. iii. La identidad del responsable del tratamiento de datos. <p>El Registro General de Protección de Datos Personales es mantenido por la Agencia Española de Protección de Datos Personales.</p>
<p>ARGENTINA Ley N° 25.326.</p>	<p>De acuerdo al artículo 13 toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.</p>
<p>COLOMBIA Ley Estatutaria 1.266</p>	<p>La Superintendencia de Industria y Comercio y la Superintendencia Financiera no llevan registro de consulta pública.</p>
<p>MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental</p>	<p>El artículo 23 dispone que los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlos de conocimiento del Instituto o de las instancias equivalente previstas en el artículo 61, quienes tienen el deber de mantener un listado actualizado de los sistemas de datos personales, y en armonía a los preceptos de la ley nada obsta a que el titular de los datos pueda solicitar su consulta.</p>

El derecho a ser informado manifestado como derecho de consulta frente a la autoridad de control refleja la necesidad de dar transparencia a los tratamientos de datos personales, mediante el cumplimiento del principio de publicidad. Sólo a través del cumplimiento de este principio se evita que existan registros de datos clandestinos

y desconocidos para los titulares de los datos, promoviéndose una fiscalización de tipo preventiva que no espera que los daños ya se hayan radicado en el afectado.

Este derecho ha sido uno de los últimos en consagrarse, frente al derecho a ser informado en caso de obtención de datos de terceros. En efecto, el Convenio 108 del Consejo de Europa no dispuso su existencia. Sólo con la Directiva 95/46 se avanzó hacia una consagración explícita de deber de los órganos de control de contar con un registro completo de los bancos de datos en manos de órganos públicos y privados, sin distinciones.

El ejercicio del derecho de consulta frente al registro de la autoridad de control no debe tener un alcance necesariamente extenso, basta que permita que el titular conozca:

- i. Si realmente existe un tratamiento de datos que le conciernan.
- ii. El nombre o dirección del responsable del banco de datos.
- iii. Los objetivos del tratamiento.
- iv. La descripción de la categoría de datos que contiene el tratamiento.
- v. Los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos.
- vi. Las transferencias de datos previstas hacia otros países.

Un aspecto importante que podría dificultar el ejercicio de este derecho es que los órganos de control deben estar provistos de recursos adecuados para hacer frente a la realización de un registro adecuado y completo; y, a una demanda creciente, por parte de los titulares de los datos, respecto a la consulta de los bancos de datos donde constan sus datos.

El Proyecto de Ley que se encuentra actualmente en el Congreso y que pretende modificar la Ley N° 19.628, resuelve varios de los problemas más profundos que aquejaban a la ley, entre los que se encuentra la inexistencia de una adecuada autoridad de control y de un registro de los bancos de datos privados. Pero

probablemente, de ser aprobado, decaiga en el ejercicio efectivo de los derechos por problemas de recursos y de una institución en marcha blanca. Aún así, el panorama es auspicioso bajo el alero de esta normativa.

Cabe señalar, sin embargo, que en cuanto al Proyecto de Ley sobre información comercial, no podemos ser tan optimistas, ya que no se cumple el principio de publicidad de los registros, pues se sustrae de los órganos de control, la facultad de llevar un catastro de los bancos de datos públicos y privados, concentrándose esta facultad en el Registro Central de Obligaciones Económicas. Este registro, lejos de ser un órgano de control, es un banco de datos oficial administrado por licitación y para acceder a la información personal siempre deberá pagarse determinada cantidad de dinero. Entendemos que la información comercial se considera un valioso recurso susceptible de evaluación pecuniaria, sin embargo, debería reconocerse al titular de los datos, al menos una vez al año, la posibilidad de saber que datos suyos se están tratando, y esta función debería entregársele al órgano de control.

5. Derecho a ser informado manifestado como derecho de rectificación, supresión y bloqueo.

PAÍS	DERECHO A SER INFORMADO MANIFESTADO COMO DERECHO DE RECTIFICACIÓN, ELIMINACIÓN O BLOQUEO
CHILE Ley N° 19.628	El artículo 12 incisos 2, 3 y 4 establece los derechos de modificación, eliminación y bloqueo que puede ejercer personalmente o debidamente representado. - Modificación: cuando los datos sean erróneos, inexactos, equívocos o incompletos, y así lo acredite el titular. - Eliminación: almacenamiento carezca de fundamento legal o cuando estuvieren caducos. - Eliminación o bloqueo: cuando el titular haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. El ejercicio de estos derechos será absolutamente gratuito, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Estos derechos deben hacerse efectivos en el plazo de dos días.
CHILE Proyecto de Ley 687-356	Se conserva el artículo 12 en su integridad pero la carga de la prueba se invierte, es decir que los datos se modifican salvo que el responsable del registro o banco de datos acredite lo contrario. Estos derechos deben hacerse efectivos en el plazo de diez días, o veinte si se trata de órganos de la Administración del Estado.
CHILE Proyecto de Ley	El artículo 17 señala que los procedimientos y plazos para ejercitar el derecho de rectificación y

sobre deuda positiva y negativa de los chilenos	cancelación serán establecidos reglamentariamente.
ESPAÑA Ley Orgánica 15/1999	El titular de los datos tendrá derecho a solicitar su rectificación y o cancelación de acuerdo a lo dispuesto en el artículo 16.2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la ley y, en particular cuando tales datos resulten inexactos o incompletos. El artículo 4.4 señala que serán sustituidos de oficio por los correspondientes datos rectificadas o completados. Estos derechos deben hacerse efectivos en el plazo de diez días. La instrucción 1/98 señala que estos derechos no tiene conexión, es decir, no son requisito previo para su ejercicio.
ARGENTINA Ley 25.326	El derecho a suprimir y rectificar datos en caso de falsedad y discriminación se contempla en el artículo 43 inciso 3 de la Constitución de Argentina. Además la ley los consagra en variados preceptos. - Suprimirlos cuando los datos sean falsos, erróneos, inexactos, inadecuados, impertinentes, innecesarios o excesivos (artículos 4.1, 4.2, 4.3, 4.4, 4.5, 4.7 y 16). Además se contemplan casos específicos en que procede el derecho a requerir supresión. - Actualización: cuando los datos estén obsoletos o vetustos (artículo 4.4) - Completar: esta hipótesis no está de forma expresa en la ley, pero puede asimilarse con la inexactitud y el error. Una vez que el responsable o usuario del banco de datos ha recibido la solicitud de rectificación, supresión, bloqueo, actualización o integración tiene cinco días hábiles para dar cumplimiento al requerimiento de titular de los datos.
COLOMBIA Ley Estatutaria 1.266	Según el artículo 6.1.1 el derecho a actualizar y rectificar los datos se ejerce frente a los operadores de los bancos de datos. El derecho a actualizar y rectificar también puede ejercerse frente a la fuente, pero ésta deberá ser reenviada al operador, pues será éste quien dé cumplimiento al derecho. Este mismo derecho procede en caso de información financiera, crediticia, comercial, de servicios y la proveniente de terceros.
MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	Según el artículo 25 señala que las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, la modificación de sus datos que obren en cualquier sistema de datos personales. El ejercicio de este derecho se realiza a través de la entrega de una solicitud de modificación a la unidad de enlace o su equivalente que señale el sistema de datos personales, las modificaciones por realizarse y la documentación que motiva la petición. El órgano tiene un plazo de treinta días hábiles para comunicar las modificaciones realizadas, o bien, se debe informar de manera fundada y motivada las razones por las que no se procedió a realizar las modificaciones.

Los derechos de modificación, eliminación y bloqueo deben garantizarse a todos los titulares de los datos, como una consecuencia del reconocimiento del principio de calidad de los datos que trascienden las leyes de protección de datos personales. Según el cual los responsables de las bases de datos tienen la obligación de garantizar la veracidad y vigencia de los datos objeto de tratamiento.

En este sentido, los datos deben ser obtenidos y tratados en forma leal y lícita, deben ser recogidos únicamente para fines determinados y legítimos, ser adecuados, pertinentes y no excesivos, exactos y actuales; y, por último, deben conservarse de tal forma y durante un período de tiempo tal que sólo permita identificar a los titulares de éstos durante el plazo necesario para el cumplimiento de los fines trazados.

En aras del cumplimiento de estos objetivos, si los titulares al conocer sus datos reconocen datos falsos, equivocados, desacertados, carentes de exactitud defectuosos e imperfectos, perciben datos sin fundamento legal que justifique su tratamiento u obsoletos o anacrónicos, o bien, ha proporcionado voluntariamente datos o éstos se utilizan para comunicaciones comerciales y no desee continuar figurando en el banco de datos definitiva o temporalmente, podrán solicitar su modificación, eliminación y bloqueo, correspondientemente.

El plazo para solicitar el ejercicio de éstos derechos es el mismo que se contempla para los casos de acceso de datos. Y de no cumplirse con lo dispuesto en la ley o evacuar un informe insuficiente, el titular de los datos podrá ejercer el recurso correspondiente.

Es importante que estos derechos contengan la obligación de hacer constar en el registro que el dato está siendo impugnado, de manera de evitar que la información en controversia se utilice para la toma de decisiones injustas que se fundamenten en datos que difieren de la realidad.

La particularidad de este derecho es que coincide con la última etapa del ejercicio del derecho de información, es decir, el sujeto ya ha tomado conocimiento sobre sus datos, a través de la información evacuada por el responsable del fichero en cualquiera de sus manifestaciones, y ha percibido que el tratamiento no está de acuerdo a derecho y debe ser enmendado para ajustarse a la ley.

6. Incumplimiento del derecho a ser informado en sus distintas manifestaciones.

PAÍS	INCUMPLIMIENTO DEL DERECHO A SER INFORMADO EN SUS DISTINTAS MANIFESTACIONES
<p>CHILE Ley N° 19.628</p>	<p>El artículo 16 establece la acción de reclamación ante los tribunales de letras civiles por incumplimiento del derecho de acceso y los derechos de modificación, eliminación y bloqueo. Esta acción procede cuando el responsable del banco de datos no se pronuncia sobre la solicitud en el plazo de dos días, o se pronuncia y la deniega, fundamentándola en causa distinta a la seguridad nacional o interés nacional (si la denegación se funda en estos motivos la acción debe presentarse ante la Corte Suprema).</p> <p>El titular tiene derecho a ser indemnizado por los daños causados, de acuerdo al artículo 23.</p> <p>Por último, la infracción a la ley de protección de datos personales, será castigada con multa de dos a cincuenta UTM, es decir, entre \$73.504 y \$1.837.600 pesos</p>
<p>CHILE Proyecto de Ley 687-356</p>	<p>El artículo 16 se reemplazo por un nuevo artículo que consagra el derecho a recurrir ante el Consejo para la Transparencia y Protección de Datos Personales. Esta acción procede cuando el responsable del banco de datos no se pronuncia sobre la solicitud en el plazo de diez días, o veinte días hábiles, tratándose de órganos de la Administración del Estado.</p> <p>El titular conserva su derecho a ser indemnizado por los daños causados pero este se traslada al artículo 27 que establece además la solidaridad del responsable del banco de datos y los cesionarios de dichos datos. Además se presume legalmente la responsabilidad del autor del daño, si existe infracción a las normas de la ley.</p> <p>Por último, la infracción a la ley de protección de datos personales, será castigada por el Consejo para la Transparencia y Protección de Datos Personales, con multa que dependerá del grado de infracción a los derechos de información:</p> <ul style="list-style-type: none"> - Para infracciones leves: multas de hasta 200 UTM, es decir, hasta alrededor de \$7.350.400. - Para infracciones graves: multas de hasta 5.000 UTM, es decir, hasta alrededor de \$183.760.000. - Para infracciones gravísimas: multas de hasta 10.000 UTM, es decir, hasta alrededor de \$367.520.000.
<p>CHILE Proyecto de Ley sobre deuda positiva y negativa de los chilenos</p>	<p>De acuerdo al artículo 15 el titular tendrá derecho a rectificar y cancelar los datos que corresponda. En la eventualidad de que la respuesta del aportante no sea satisfactoria podrá recurrir dentro del plazo de quince días, contado desde la notificación de la respuesta, al Consejo de Transparencia y Protección de Datos Personales, ajustándose al procedimiento que contempla la misma indicación sustitutiva, procediendo recurso de ilegalidad ante la Corte de Apelaciones.</p> <p>Según el artículo 16 los afectados como consecuencia del incumplimiento tendrán derecho a ser indemnizados por las entidades fiscalizadas responsables del tratamiento de datos, presumiéndose legalmente la responsabilidad del autor del daño, si existe infracción a las normas de la ley.</p> <p>El proyecto establece sanciones al incumplimiento de los principios y tangencialmente al derecho a ser informado en sus distintas modalidades, fijando sanciones leves, graves y gravísimas por los mismos montos del proyecto 687-356.</p>
<p>ESPAÑA Ley Orgánica</p>	<p>El artículo 18 establece la acción de reclamación frente a la Agencia de Protección de Datos por incumplimiento a la normativa.</p> <p>EL artículo 19 consagra el derecho a ser indemnizado como consecuencia del incumplimiento.</p>

15/1999	<p>Por último, se establecen sanciones para las infracciones leves, graves y gravísimas:</p> <ul style="list-style-type: none"> - Las infracciones leves son sancionadas con multa de 100.000 a 10.000.000 de pesetas, es decir, alrededor de \$424.348 a \$42.458.322. - Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas, es decir, alrededor de \$42.458.322 a \$212.289.011. - Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas, es decir, alrededor de \$212.289.011 a \$424.580.702.
<p>ARGENTINA Ley N° 25.326</p>	<p>La acción de hábeas data que contempla la ley argentina del artículo 33 y siguientes, se ejerce ante el juez del domicilio del demandado. La competencia federal procede cuando se interponga contra archivos públicos de organismos nacionales y cuando los archivos de datos se encuentren interconectados en redes jurisdiccionales, nacionales o internacionales. No se establece un recurso frente a la denegación de la solicitud frente al organismo de control, sólo se señala que el organismo de control deberá llevar un registro y que en caso de rechazo de la acción, ésta no constituye presunción de responsabilidad en que hubiera podido incurrir el demandante.</p> <p>En cuanto a las sanciones administrativas que se derivan del incumplimiento, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos a cien mil pesos, clausura o cancelación del archivo, registro o banco de datos. Las multas equivalen a \$134.467 hasta \$13.446.707.</p>
<p>COLOMBIA Ley Estatutaria 1.266</p>	<p>De acuerdo al artículo 16.6 sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida.</p> <p>El incumplimiento del derecho de información no encuentra una sanción específica, de manera que la sanción deberá regularse por la Superintendencia correspondiente, dentro del marco trazado que establece las siguientes sanciones:</p> <ul style="list-style-type: none"> - Multas de hasta mil quinientos salarios mínimos, que traducidos a pesos chilenos corresponden a alrededor de \$212.272.000. - Suspensión de las actividades del banco de datos hasta por un término de seis meses. - Clausura temporal o definitiva de las operaciones del banco de datos en los casos más graves.
<p>MÉXICO Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental</p>	<p>El artículo 50 establece un recurso de revisión que debe interponerse dentro de los quince días hábiles siguientes a la fecha de la notificación, ante el Instituto o ante la unidad de enlace que haya conocido el asunto. El recurso procederá por las siguientes causales:</p> <ol style="list-style-type: none"> i. Negativa de entregar o corregir datos personales. ii. Falta de respuesta en los plazos señalados. <p>Serán causa de responsabilidad administrativa:</p> <ul style="list-style-type: none"> - Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a la ley. - Denegar intencionalmente información no clasificada como reservada o no considerada confidencial conforme a la ley. - Entregar intencionalmente de manera incompleta información requerida en una solicitud de acceso (conducta considerada grave para efectos de su sanción administrativa). - No proporcionar la información cuya entrega haya sido ordenada por los órganos o el Poder Judicial de la Federación.

Hasta aquí, hemos hecho presente el trabajo de codificación de los países estudiados, dirigido principalmente a consagrar importantes derechos substantivos. Falta, sin embargo, otorgar a estos derechos un campo de acción expedito y obtener de ellas todo el fruto que deben rendir, dotándolas de procedimientos adecuados para el ejercicio y salvaguardia de los derechos cuando éstos han sido vulnerados.

Las hipótesis de incumplimiento dicen relación con la negativa de los responsables del tratamiento de datos frente a los deberes de informar de oficio, a satisfacer el ejercicio de los derechos de acceso, modificación, eliminación y bloqueo, a enlistarse en los registros nacionales a cargo de la autoridad de control; y, en general, cualquier comportamiento que genere inobservancia a los preceptos que protegen los derechos de los datos personales y que se vinculan al derecho a ser informado en cualquiera de sus manifestaciones.

Hemos visto que los incumplimientos del responsable del fichero pueden generar la interposición de las acciones legales correspondientes frente a la autoridad de control, o frente a los tribunales de justicia, según lo que dispongan las leyes de cada país, sin perjuicio, de la acción indemnizatoria que podrá ejercerse ante la justicia ordinaria. No obstante, el régimen que ha adoptado cada país es bastante variable. Algunos han preferido mantener la competencia de los tribunales ordinarios en el ejercicio de la acción de hábeas data, otros han considerado su competencia sólo como un recurso que se concede una vez intentada la vía directa frente al responsable y ésta ha fracasado. Por último, otros han optado por concentrar todas estas facultades en el órgano de control, es decir, entregándole competencia para conocer los conflictos entre titulares de datos y responsable de registros cuando hay incumplimiento a los derechos de acceso, modificación, eliminación y bloqueo de datos.

Si se aprueba el Proyecto de Ley que modifica la Ley N° 19.628 nuestro sistema transitaría de un extremo al otro. Es decir, actualmente si el titular de los datos ha visto vulnerado sus derechos, podrá ejercer el derecho de reclamación contemplado, o bien, interponer un recurso de protección, fundado en transgresión al artículo 19 N° 4 que protege la vida privada. Si se aprobará la ley, el titular debería dirigirse al Consejo para

la Transparencia y la Protección de Datos Personales, una vez fracasada la solicitud frente al responsable del banco de datos.

La posibilidad de contar con una consagración de esta naturaleza es una iniciativa que debe aplaudirse. Un sistema de esta categoría permitiría el reconocimiento de la protección de datos personales como un área específica e independiente que requiere competencia jurisdiccional especial que permita la resolución de los conflictos en un nivel de conocimiento adecuado. Justamente, el contar con un órgano específico que trate las temáticas de protección de datos personales, de manera similar al Tribunal de la Libre Competencia o al Tribunal de la Contratación Pública, posibilitaría la existencia de una instancia especial e independiente, que se dedique exclusivamente al conocimiento de aquellas materias vinculadas a la protección de datos personales.

Sin embargo, no debe olvidarse que el emprendimiento de un propósito de esta magnitud peca de un optimismo excesivo. El Consejo para la Transparencia fue creado para finalidades distintas a las que pretende atribuirle la modificación a la Ley N° 19.628, atribuyéndosele más de una decena de facultades cuyo objetivo principal es satisfacer las necesidades de transparencia de los órganos del Estado frente a la sociedad. Sólo una de estas facultades se refiere a la cautela del cumplimiento de la Ley N° 19.628 de Protección de Datos de carácter Personal por parte de los órganos de la Administración del Estado.

Por lo tanto, no sería extraño que el Consejo para la Transparencia se vea superado en sus tareas asignadas, tras la posible aprobación del Proyecto de Ley moción 687-356. Al observar la experiencia de las autoridades de control que se han creado, específicamente para la protección de datos personales, en cuyos casos estas autoridades no han adquirido competencia por ampliación de las facultades sino que la poseen originalmente, ya se han revelado serios problemas de recursos y competencias necesarias para garantizar la aplicación efectiva de la legislación sobre protección de datos.

Esta situación no se aparta de lo que ha ocurrido en países latinoamericanos. A finales de 2003 la prensa argentina informó a la Dirección de Protección de Datos Personales de ese país que estaba colapsada y que circulaban prácticamente sin control más de cien mil bases de datos personales que incluían desde informes crediticios ilegales hasta las ventas de bases de datos a gobiernos extranjeros, pasando por el telemarketing sin consentimiento de quienes reciben las consultas y el envío de e-mails masivos sin detalles de procedencia. Además se destaca que desde que se reformó la Constitución en 1994 y se creó la figura del hábeas data en 1995 no se le da dado la real importancia al tema y los sucesivos presidentes no han hecho más que crear la Dirección Nacional de Protección de Datos Personales, con mínima estructura¹²⁴.

Cabe preguntarse entonces, cuáles son los pronósticos para un órgano que fue creado para una finalidad distinta, y al cual se le agregan competencias y facultades dado el contexto de necesidad en que se encuentra la protección de datos personales. Quizás sería más apropiado crear un órgano específicamente para la protección de los datos personales y asumir que en sus comienzos podrá tener debilidades como cualquier institución que comienza su marcha blanca, falencias que podrán superarse con el correr del tiempo, el trabajo arduo y el consecuente fortalecimiento de la estructura dispuesta en la ley.

En cuanto a la fiscalización que ejercen los órganos de control en materia de tratamiento de datos personales, gran parte se realiza a través de un sistema de tipificación de conductas infractoras que pueden ser sancionadas administrativamente por el propio organismo de control, sin recurrir para ello a los tribunales de Justicia. Ya vimos como el establecimiento de estas sanciones ha variado mucho en las diferentes legislaciones estudiadas. Sólo la legislación española y, eventualmente, la chilena, de

¹²⁴ Circulan casi sin control los datos personales: La dependencia que fiscaliza el manejo de la información privada está colapsada. Artículo publicado en La Nación On Line el 28 de julio de 2003. http://www.lanacion.com.ar/03/07/28/dp_514770.asp.

llevarse a aprobar el Proyecto de Ley, contemplan sanciones específicas para los casos de incumplimiento de los deberes de información en sus distintas modalidades.

La mayor importancia de estos sistemas sancionatorios se centra en el rol disuasivo que juegan estas prescripciones frente a los responsables del tratamiento de datos personales. La idea, es que a través de la tipificación de conductas infractoras y su pena pecuniaria asociada, se logre retraer a los actores de un posible incumplimiento. Así, el monto sólo atenderá a la real posibilidad de que los responsables de los bancos de datos estimen más rentable ajustarse a la normativa que dejar de cumplirla. En este sentido, los montos establecidos por el proyecto son bastante adecuados, pues de acuerdo al régimen actual, la desvinculación respecto a la ley, está asegurada.

Tras este análisis podemos concluir que la regulación de los principios y criterios generales en materia de control de datos y específicamente en los derechos de los titulares a ser informados, consagrados en la actual Ley de Protección a la Vida Privada, están lejos de solucionar las falencias que nuestra nación posee. La sola regulación de éstos no basta para crear una estructura suficiente capaz de sustentar un completo sistema de protección de datos personales en cuya base se encuentre el derecho del titular a ser informado.

Todos los principios se desvanecen si no se adopta un adecuado sistema de responsabilidad que sea capaz de sancionar los incumplimientos de manera de desincentivar las conductas lesivas de derechos personales. Precisamente esta es la debilidad fundamental de la Ley N° 19.628, ya que efectivamente contempla la existencia de algunos derechos de información, planteados de manera imperfecta pero proclamados al fin y al cabo. Sin embargo, de nada sirven estos derechos si no se dispone de un organismo de control que fiscalice el mercado de circulación de datos, sancione a los infractores y permita el ejercicio de estos derechos.

Un último punto importante a recalcar respecto al ejercicio de los derechos de información como control de datos personales consiste en que su desenvolvimiento depende en gran medida, también, del grado de conocimiento que tienen los

individuos respecto a este tema. Es decir, debiera avanzarse hacia una educación de la población que le enseñe los derechos que le asisten y como ejercerlos. Hoy existe una gran ignorancia respecto al tratamiento de datos personales de los individuos, los que no dimensionan a qué nivel pueden ser transgredidos sus derechos.

BIBLIOGRAFÍA

AGENCIA DE PROTECCIÓN DE DATOS. Tratamiento de datos personales informatizados, Madrid, 1995, p138.

AGUILERA, Abel Téllez, “Nuevas tecnologías. Intimidad y Protección de Datos”, Madrid, Edisofer, 2001, 435p.

ÁLVAREZ González, Susana, Derechos fundamentales y protección de datos genéticos, 1º Edición, Instituto de Derechos Humanos Bartolomé de las Casas, Universidad Carlos III de Madrid, 2007, 534p.

ANGUITA Ramírez, Pedro, La Protección de Datos Personales y el Derecho a la Vida Privada, Régimen Jurídico, Jurisprudencia y Derecho Comparado, Santiago, Editorial Jurídica de Chile, 2007, 627p.

ARENAS Ramiro, Mónica, El derecho fundamental a la protección de datos personales en Europa, Valencia Tirant Lo Blanch, 2006, 638p.

ARMAGNAGUE, Juan, Derecho a la información, Hábeas Data e Internet, Buenos Aires, Ediciones La Roca, 2002, 592p.

BERTELSEN Repetto, Raúl, Datos personales: Propiedad privada, libre iniciativa particular y respeto a la vida privada, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobreprotección de datos de carácter personal, Universidad de Los Andes, 2001, 113-129.

BIANCHI, Alberto, Hábeas Data y Derecho a la privacidad, en Revista Jurídica El Derecho, tomo 160 – 866, Buenos Aires.

BING, Jon, Derecho a la información: Una breve introducción, en Revista *Ágora*, N°6, 1983, 35p.

BOLOTNIKOFF, Pablo, Informática y responsabilidad civil: contratos informáticos, bases de datos, nombres de dominio de Internet, contenidos ilícitos en Internet, contratación electrónica y firma digital, 1° Edición, La Ley, Buenos Aires, Argentina, 2004, 371p.

CASTILLO Jiménez, Cinta, Las nuevas tecnologías de la información y el derecho de Vittorio Frosini a Internet, Instituto de Estadística de Andalucía, Consejería de Economía y Hacienda, Sevilla, 2003, 183p.

CERDA Silva, Alberto, La autoridad de control sobre protección de datos personales, en *Anales de la Facultad de Derecho*, Santiago, Universidad de Chile, núm. 2, 2005, 35-68p.

CERDA Silva, Alberto, Mecanismos de control en la Protección de Datos Personales en Europa, en *Revista Ius et Praxis*, Derecho de la Región, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Talca, 2006, 221-251p.

CERDA Silva, Alberto, Hacia un modelo integrado de regulación y control en la protección de datos personales, en *Revista de Derecho y Humanidades/ N° 13*, 2008, Santiago, 121-130p.

COMISIÓN NACIONAL PARA EL MEJORAMIENTO DE LA ADMINISTRACIÓN DE JUSTICIA, Informática y derecho a la intimidad. Perspectivas de política criminal, en *Revista Judicial*, Costa Rica Año XVI, N°53, 1991, 136p.

DEFENSORÍA DEL PUEBLO COLOMBIANO, Memorias del foro sobre Protección de datos Personales y Regulación Legal del Hábeas Data, Dirección Nacional de Promoción y Divulgación de Derechos Humanos, Bogotá, 2004, 196p.

DESANTES Guanter, José María, La información como derecho, Madrid, Editorial Nacional, 1974, 31p.

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), Privacy & Human Rights: An international survey of privacy laws and development, Washington, EEUU, 2002.

JIJENA Leiva, Renato, La ley chilena de protección de datos personales. Una visión crítica desde el punto de vista de los intereses protegidos, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobreprotección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, 85-110p.

FORD, Aníbal, La marca de la bestia. Identificación, desigualdades e infoentretenimiento en la sociedad contemporánea, Buenos Aires, Grupo Editorial Norma, 1999.

FREIXAS Gutiérrez, G., La protección de los datos de carácter personal en el derecho español, Barcelona, Bosh, 2001, 394p.

FROSINI, Vittorio, La tutela de la privacidad de la libertad informática al bien jurídico informático, Revista de Colegio de Abogados, Buenos Aires, 1989.

GILS CARBÓ, Alejandra, Régimen legal de las bases de datos y hábeas data, Buenos Aires, La Ley, 2001, 355p.

GÓNZÁLEZ Hoch, Francisco, Modelos comparados de protección, en obra colectiva Tratamiento de datos personales y protección de la vida privada, Estudios sobre la Ley N° 19.628 sobreprotección de datos de carácter personal, Santiago, Universidad de Los Andes, 2001, p153-178.

GOÑI SAIN, José Luis, La videovigilancia empresarial y la protección de datos personales, Madrid, Thomson-Civitas, 254p.

HASSEMER, Winfried y Chirino Sánchez, Alfredo, El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales, Buenos Aires, Editores del Puerto, 1997, 238p.

HERRÁN Ortiz, Ana Isabel, El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales, Madrid, Editorial Dykinson, 2002, 388p.

HERRERA Bravo, Rodolfo, Consideraciones sobre la dialéctica y el equilibrio entre la información pública y los datos personales, en Revista de Derecho Universidad Viña del Mar Nomos, Viña del Mar, Segundo Semestre 2008, 161-182p.

JERVIS Ortiz, Paula, Modelo de Propuesta Regulatoria al Mercado de Datos Personales en Chile, en Revista Chilena de Derecho Informático N° 8, Centro de Estudios en Derecho Informático, Universidad de Chile, Facultad de Derecho, 2006, 151-175p.

LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática, Madrid, Tecnos, 1990, 207p.

LUCAS MURILLO DE LA CUEVA, Pablo, La construcción de derecho a la autodeterminación informativa, Revista de estudios políticos, ISSN 0048-7694, N° 104, 1999, Madrid, 35-60.

LUCAS MURILLO DE LA CUEVA, Pablo, Informática y Protección de Datos Personales, Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, Centro de Estudios Constitucionales, Madrid, 165p.

MARTÍNEZ Martínez, Ricardo, Una aproximación crítica a la autodeterminación informativa, Thompson Civitas Ediciones, Madrid, 2004, 403p.

MATUS Arenas, Jessica, El deber de información y el consentimiento para la cesión de datos personales, Lexis Nexis, Santiago, 2006, 176p.

ORTIZ, Claudio, La protección de datos personales y la información comercial, en obra colectiva Chile y la protección de datos personales ¿Están en crisis nuestros derechos fundamentales?, Santiago, Serie Políticas Públicas, 2009, 23-35.

ORTÍZ Ortíz, Rafael, Hábeas data: derecho fundamental y garantía de protección de los derechos de la personalidad, Caracas, 2001, 967p.

PÉREZ LUÑO, A.E.: Comentario legislativo: La LOARTAD y los derechos fundamentales, Madrid.

RUIZ, Miguel Carlos, La configuración constitucional del derecho a la intimidad, Madrid, Tecnos, 1995, p.379.

SANZ – MAGALLÓN, José María, “¿Qué es la Sociedad del Conocimiento?”, en Nueva Revista de Política, Cultura y Arte, 9-15:, Madrid, 2000.

SERRANO Pérez, María Mercedes, El derecho fundamental a la protección de datos. Derecho español y comparado, Madrid, Thompson, Civitas, 2003, 518p.

TRUYOL Serra, Antonio, “Bases filosóficas y metodológicas para un derecho de la sociedad de la información” en la obra colectiva Implicaciones socio-jurídicas de las tecnologías de la información, Madrid, CITEMA, 1991, pp139-143.

VARIOS AUTORES, Ius et Praxis: derecho en la región, Derecho a la autodeterminación informativa y acción de Hábeas Data en Iberoamérica, Talca, 1997.

VIAL CLARO, FELIPE. Tratamiento de datos personales y protección de la vida privada: estudios sobre la ley no. 19.628 sobre protección de datos de carácter personal, Santiago, 2001, p178.

WARREN, S. D. y Brandeis L. D., The right to privacy, en Harvard Law Review, vol. IV, núm. 5, diciembre de 1890, p.193-220.

LEYES

Ley N° 19.628 sobre Protección de la Vida Privada, Ministerio Secretaria General de la Presidencia, Santiago, Chile, 28 de agosto de 1999.

Ley Orgánica 15/1999 sobre Protección de Datos de Carácter Personal, Madrid, España, 13 de diciembre de 1999.

Ley 25.326 sobre Protección de los Datos Personales, Buenos Aires, Argentina, 4 de octubre de 2000.

Disposición N° 7/2005. Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante violaciones a las normas de la Ley N° 25.326 y de las reglamentaciones dictadas en su consecuencia. Derógase la Disposición N° 1/2003.

Ley Estatutaria 1.266 por la cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, Bogotá, Colombia, 31 de diciembre de 2008.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ciudad de México, México, 11 de junio de 2002.

TRATADOS INTERNACIONALES

Convenio N° 108 del Consejo de Europa de 28 de enero de 1981 de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

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.

PROYECTOS DE LEY

Proyecto de Ley, Mensaje N° 687 – 356 de S.E. la Presidenta de la República con el que inicia el Proyecto de Ley que introduce modificaciones a la Ley N° 19.628 y a la Ley 20.285, Santiago, Chile, 26 de agosto de 2008, Pág. 2.

Proyecto de Ley N° 293-357, Formula indicación sustitutiva a los Proyectos de Ley que modifican la Ley N° 19.628 sobre Protección a la Vida Privada (Boletines N° 5309-03, 5356-07 y 6298-05), Santiago de Chile, 8 de mayo de 2009.

ARTÍCULO DE DIARIO

Peter Hill: "No estamos de acuerdo con que la base de datos (...) vaya a dar a un ente estatal", Entrevista, El Mercurio, martes 12 de mayo de 2009.

DOCUMENTOS E INFORMES

Actas Oficiales de la Comisión Constituyente, volumen 3, Garantías Constitucionales, Sesiones 128° de 10 de junio de 1975, 129° de 12 de junio de 1975 y 130° de 17 de junio de 1975, Santiago.

TEXTOS ELECTRÓNICOS, BASES DE DATOS Y PROGRAMAS INFORMÁTICOS

https://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/index-ides-idphp.php

http://www.madrid.org/cs/Satellite?cid=1247227049247&language=es&pagename=PortalAPDCM%2FPAGE%2FPAPD_listado

COOPERATIVA.CL, tópicos economía, nacional, endeudamiento, Proyectos de Ley sobre datos personales protegen al consumidor, destacó Hacienda [En línea], Santiago, 12 de mayo de 2009, http://www.cooperativa.cl/proyectos-de-ley-sobre-datos-personales-protegen-al-consumidor--destaco-hacienda/prontus_notas/2009-05-12/073335.html [Consulta 10 de julio de 2009]

REVISTA LA PÁGINA, Traspaso de diagnósticos: Violación a nuestra privacidad [en línea], Santiago, 2 de junio de 2009, <http://revistalapagina.com/2009/06/02/aspaso-de-diagnosticos-violacion-a-nuestra-privacidad/>

Circulan casi sin control los datos personales: La dependencia que fiscaliza el manejo de la información privada está colapsada. Artículo publicado en La Nación On Line el 28 de julio de 2003. http://www.lanacion.com.ar/03/07/28/dp_514770.asp.