PROTECCIÓN DE DATOS EN CHILE A LA LUZ DE LA DIRECTIVA DE LA UNIÓN EUROPEA

CHRISTIAN SCHMITZ VACCARO*

RESUMEN

El propósito del presente trabajo es entregar una visión acerca de la protección de datos personales en Chile, calificándola a la luz de los estándares internacionales, específicamente europeos. Al efecto, se contrasta la legislación chilena de protección de datos con una norma modelo, como lo es la Directiva 95/46/CE 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.

El trasfondo de dicho estudio está constituido por las crecientes necesidades de que nuestro país, adopte niveles mínimos de protección de datos personales, dada la mayor integración de Chile en las redes económico-comerciales que imperan entre los países (tratados de libre comercio) y que no sólo involucran productos, sino también los servicios.

Palabras o conceptos claves: *protección de datos personales.*

ABSTRACT

The purpose of this work is to present a vision and an evaluation of personal data protection in Chile in relation to international standards, specifically the European ones. In this regards the Chilean legislation of personal data protection is compared to a legal pattern, which is Directive 95/46/CE, of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The background of this research is based on a growing need of our country to implement minimum levels of personal data protection, due to Chile's integration in economic and commercial networks with other countries (free trade agreements), involving not only products but also services.

Keywords: *personal data protection.*

* Abogado MBA-UC. Profesor de Derecho Económico y Derecho Informático. Universidad Católica de la Santísima Concepción. Universidad San Sebastián, Sede Concepción.

1. INTRODUCCIÓN

Desde ya algún tiempo, se puede observar una toma de consciencia de temas relacionados con la protección de datos. Así se ha llegado, también en nuestro país, a legislar acerca de la vida privada. Pese a ello persisten necesidades para que naciones, como Chile, adapten niveles mínimos de protección de datos personales. Ello principalmente por dos razones.

Por un lado, resulta claro que con el avance y auge de las tecnologías de la información y de las telecomunicaciones, el procesamiento y seguimiento de las personas y de sus datos se ha facilitado enormemente, lo cual ha conllevado a un notable incremento de tales actividades. Al mismo tiempo, la información que a través de dichos medios tecnológicos es posible recabar, constituye un preciado activo, tanto para las empresas en lo que se refiere a sus posibilidades de negocios, como para el Estado, como ente controlador de la vida de sus ciudadanos.

Por otra parte, el tejido de redes internacionales en los más diversos ámbitos (económicos, políticos, sociales, culturales, etc.), llamado comúnmente "globalización", conduce a un creciente intercambio transfronterizo de datos que hacen más vulnerables a las personas en lo que se refiere a un mínimo resguardo de su vida privada e intimidad.

Son estas consideraciones que se han tomando en cuenta cuando en 1995, la Unión Europea aprobó la Directiva 95/46/CE 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. En dicho cuerpo normativo se contienen disposiciones que tienen incidencia más allá de las fronteras comunitarias. Nos referimos específicamente al capítulo IV sobre "Transferencia de Datos Personales a Países Terceros" (arts. 25 y 26), así como a los preceptos sobre el "Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales", comúnmente llamado "Grupo del Artículo 29"[1] (arts. 29 y 30).

El artículo 25 de la Directiva establece como principio básico que los Estados miembros sólo podrán autorizar transferencias de datos personales a terceros países, si éstos garantizan un nivel adecuado de protección. El "carácter adecuado del nivel de protección" deberá evaluarse caso a caso "atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos". La Comisión Europea podrá declarar que determinados países ofrecen una protección adecuada.

En lo relativo al Grupo del artículo 29, es menester tener en cuenta que dentro de sus funciones se contempla la revisión periódica de la situación de protección de datos en terceros países, informando al respecto a las instituciones comunitarias.[2]

Con lo anterior queda claro la trascendencia que tiene el hecho de pertenecer al "grupo privilegiado" de países que aseguran un nivel mínimo de protección, lo cual evidentemente facilita no sólo la transferencia de datos personales entre la Unión Europea y dichos países, sino que en general, las relaciones bilaterales en los ámbitos económicos y políticos.

Considerando que Chile firmó ya hace algún tiempo un Acuerdo de Asociación con la Unión Europea, podemos señalar que resulta aún más apremiante la necesidad de que nuestro país se alinee entre los países que cuenten con un nivel apropiado de protección de datos personales. Es más, tal como lo veremos más adelante, el propio tratado contiene normas sobre el tema.

En el presente estudio sobre la situación chilena de la protección de datos, seguiremos la pauta de trabajo que el Grupo del Artículo 29 generalmente adopta en sus informes. Esta estructura muy clara y lógica se encuentra contenida en el Documento de Trabajo titulado "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre

[1] El Grupo de Trabajo, creado por el artículo 29 de la Directiva 95/46/CE, es un órgano consultivo independiente de la UE sobre protección de datos y vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

[2] Artículo 30 apartado 1, letra b) y apartado 6 de la Directiva.

protección de datos de la UE", aprobado por el Grupo el 24 de julio de 1998[3]. En consecuencia, describiremos el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz, lo cual se traduce en analizar los siguientes ítems: marco jurídico y ámbito de aplicación, principios sustanciales y mecanismo de aplicación de las herramientas legales disponibles.

2. MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS EN CHILE

El contexto jurídico actual de la protección de datos en nuestro país, está conformado por normas constitucionales, legales y reglamentarias.

La Constitución Política de 1980 no alude en forma directa al tema de la protección de datos personales, sino que sólo lo consagra tácitamente dentro de las siguientes derechos fundamentales:

- el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia (art. 19 n° 4),
- la inviolabilidad del hogar y de toda forma de comunicación privada (art. 19 n° 5), y
- la libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio (art. 19 n° 12).

En el plano legal, la normativa principal sobre protección de datos se encuentra contenida en la Ley 19.628, titulada "ley sobre Protección de la Vida Privada". Dicha ley, pese a su título amplio, regula "únicamente" aspectos sobre "el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares".[4]

Con esta ley, publicada el 28 de agosto de 1999 en el Diario Oficial, Chile se convirtió en uno de los primeros países dentro de Latinoamérica en abordar esta temática tan trascendental para la vida en sociedad. Hasta la fecha, la Ley 19.628 ha sido modificada una sola vez; en efecto la Ley 19.812[5], introdujo cambios menores, habiendo sido su objetivo principal, la eliminación de datos de morosidades históricas y con ello la reinserción crediticia y laboral de una parte importante de la población.

Por su parte, la Ley 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo (Publicada en el Diario Oficial del 4 de junio de 2001) regula las funciones de los medios de comunicación social, estableciendo el marco de su ejercicio legítimo.

Por último, cabe incluir en esta enumeración normativa, el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos, aprobado mediante el Decreto nº 779 del Ministerio de Justicia (Diario Oficial del 11 de noviembre de 2000).

En el contexto del presente trabajo, resulta además interesante referirse al Acuerdo de Asociación entre la Unión Europea y Chile, firmado a fines del año 2002. Dicho tratado contempla dos disposiciones que aluden directamente a la cooperación en materia de protección de datos[6]:

[3] Dicho documento se encuentra contenido en el *"Working Paper 12"* del Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/wp12_es.pdf

[4] Art. 1 de la Ley 19.628 sobre Protección de la Vida Privada.

[5] Dicha ley, que fue publicada en el Diario Oficial del 13 de junio de 2002, también es conocida como "Ley Dicom", nombre éste que corresponde a la principal empresa chilena responsable de bases de datos de informaciones comerciales y financieras (Dicom es una empresa dependiente de la multinacional Equifax Inc.).

[6] Sin perjuicio de las dos disposiciones transcritas, hacen referencia al tema además las siguientes artículos: 41.3 letra b), 117.9 xv), 122 y 135.1 letra e).

Artículo 30 *"Protección de datos*
1. Las Partes acuerdan cooperar en la protección de los datos personales para mejorar el nivel de protección y evitar los obstáculos al comercio que requiera la transferencia de datos personales.
2. La cooperación en el ámbito de la protección de datos de carácter personal podrá incluir asistencia técnica mediante intercambio de información y de expertos, y la creación de programas y proyectos conjuntos."

Artículo 202 "*Protección de datos*
Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales."

Particularmente, esta última norma compromete a las partes, en especial a la chilena, con la implementación de estándares de protección de datos que cumplan las exigencias impuestas por cuerpos normativos avanzados en la materia. Al respecto, se nombra comúnmente como ley modelo a la Directiva 95/46/CE 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. Cabe añadir, que hasta la fecha no ha habido modificaciones que denoten la materialización del compromiso referido.

Ámbito de Aplicación de la Ley de Protección de la Vida Privada.
Con base en el marco jurídico esbozado anteriormente, es posible delinear el ámbito de aplicación de nuestra legislación. Este se encuentra especificado en el artículo 1° de la Ley 19.628, comprendiendo "el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares".

Teniendo en cuenta esta disposición, es posible distinguir un ámbito objetivo y un ámbito subjetivo de aplicación de la ley.[7] El ámbito objetivo está conformado por el tratamiento de datos personales incluidos en registros o bancos de datos. La ley entrega algunas definiciones aclaratorias al respecto:

- *Datos de carácter personal* o *datos personales*, son "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables."
- *Tratamiento de datos*: "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma."
- *Registro o banco de datos*: "el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos."[8]

Al tenor del mismo precepto antes citado, quedan expresamente excluidos del régimen de dicha ley, el tratamiento de datos personales:
- que se encuentran aislados, es decir se trata de datos que no están organizados en un registro o banco de datos, y
- que se efectúe en ejercicio de las libertades de emitir opinión y de informar. Ello garantizará un amplio margen de acción a los medios de comunicación social.

[7] Esta distinción fue realizada por: Jervis Ortiz, Paula, ***"Intimidad y Nuevas Tecnologías"***, ponencia del Congreso Preparatorio del X Congreso Iberoamericano de Derecho e Informática, 13 de agosto de 2003, Santiago de Chile.
[8] Ley 19.628, artículo 2, letra f), o) y m), respectivamente.

En lo relativo al ámbito subjetivo de aplicación de la ley, las normas tienen diversos destinatarios:

- *Responsable del registro o banco de datos*, entendiéndose por tal "la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal",[9]
- *Titular de datos personales*, el que por imperativo legal es únicamente "la persona natural a la que se refieren los datos de carácter personal."[10] En consecuencia, quedan expresamente excluidas las personas jurídicas como sujeto de protección de datos personales.[11]
- *Autoridad de Registro*, función que la ley entrega en forma muy limitada al Servicio de Registro Civil e Identificación, entidad que llevará un registro de los bancos de datos personales a cargo de organismos públicos.[12]
- *Terceros a quienes se comunican datos*, son las personas distintas del titular de los datos, sean determinadas o indeterminadas, a los cuales se les da a conocer de cualquier forma datos de carácter personal.

3. EVALUACIÓN DE LA LEGISLACIÓN CHILENA EN BASE A LA DIRECTIVA DE LA UE

Con el objeto de calificar de adecuado o no el nivel de protección de nuestra legislación de protección de datos, efectuaremos a continuación una evaluación de la Ley 19.628 sobre protección de la vida privada, contrastándola con la Directiva 95/46/CE 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.

Tal como ya hemos advertido, estructuraremos este análisis de acuerdo a la pauta del Documento de Trabajo "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", el cual se expresa en los siguientes términos: "tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un 'núcleo' de principios de 'contenido' de protección de datos y de requisitos 'de procedimiento/de aplicación', cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección."[13]

3.1. *Principios consagrados por la Legislación Chilena*

Se distinguen por una parte, principios sustanciales o de contenido que son aplicables a todo tipo de tratamiento de datos, y por la otra principios específicos o adicionales, que se refieren sólo a algunos tipos específicos de tratamiento. Trataremos a continuación ambas clases de principios en el orden enunciado.

3.1.1. *Principios sustanciales consagrados por la Legislación Chilena*

De acuerdo con el documento de trabajo antes citado, se detallan los siguientes principios sustanciales o de contenido:

[9] Artículo 2, letra n) de la Ley 19.628.
[10] Artículo 2, letra ñ) de la Ley 19.628.
[11] Actualmente se encuentran en trámite dos proyectos de ley que proponen modificar este aspecto, haciendo extensiva la protección de la ley 19.628 a las personas jurídicas.
[12] Artículo 22 de la Ley 19.628.
[13] Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, *"Working Paper 12"*, ob. cit.

"1) *Principio de limitación de objetivos* - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.

2) *Principio de proporcionalidad y de calidad de los datos* - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos en relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) *Principio de transparencia* - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2 y 13 de la Directiva.

4) *Principio de seguridad* - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del mismo, no debe tratar los datos salvo por instrucción del responsable.

5) *Derechos de acceso, rectificación y oposición* - el interesado debe tener derecho a obtener una copia de todos los datos relativos a él, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

6) *Restricciones respecto a transferencias sucesivas a otros terceros países* - únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva."

Veremos a continuación, en qué medida la ley chilena consagra dichos principios básicos.

El primer principio – *el de limitación de objetivos*, también llamado principio de finalidad – se encuentra recogido por la ley chilena, al exigirse que "la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público."[14]

Por otra parte, el artículo 9 (inc. 1°) prevé que "los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público." Para comprender el real significado de esta norma, se hace necesario recurrir a la definición legal de "fuentes accesibles al público", entendiéndose por tal "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes."[15]

[14] Artículo 4, inciso 2° de la Ley 19.628.
[15] Artículo 2, letra i) de la Ley 19.628.

A diferencia de lo que sucede en el derecho comparado, la definición que la ley chilena efectúa de fuentes accesibles al público, carece de precisión. En efecto, se echa de menos una enumeración más o menos taxativa, como por ejemplo la que realiza la ley española (LOPD, art. 3 letra j). Como consecuencia, el concepto no queda claramente circunscrito y adopta un carácter bastante flexible, acorde a las conveniencias del caso particular. Resulta entonces que son los tribunales, los llamados a esclarecer si un dato determinado proviene o no de una fuente accesible al público.[16]

En este mismo contexto, no podemos sino estar plenamente de acuerdo con la critica formulada por el autor Rodolfo Herrera, al sostener que "el principio de finalidad [...] se desarrolla a lo largo de la Ley sin la fuerza suficiente, y ello [...] porque no exige que la finalidad sea determinada y explícita, y porque, [...] abre la posibilidad de que los datos puedan seguir una finalidad distinta a la que motivó la recogida, al exigir que, respecto de la transmisión de datos a través de una red digital, dicha comunicación guarde relación con las finalidades tanto del cedente como del cesionario. Así, sin existir una limitación legislativa, el tenor literal de la Ley admite la posibilidad de que el organismo requirente persiga un propósito diverso al del responsable del registro que almacena el dato."[17]

En lo que ataña al *principio de calidad de los datos,* el artículo 9 en su inciso 2° establece lo que ha de entenderse por calidad de datos: "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos." Lo anterior debe complementarse con los derechos a rectificación (o modificación) o a cancelación (o eliminación) que la ley entrega al titular de los datos. El primer derecho procede "en caso que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite", y el segundo cuando el almacenamiento de los datos "carezca de fundamento legal o cuando estuvieren caducos."[18]

Por su parte, el *principio de proporcionalidad,* que se refiere a que los datos recopilados o transmitidos deben guardar un grado de relación con el objetivo del tratamiento, sólo se encuentra establecido en forma deficiente e incompleta en Chile. La única disposición que alude a dicho principio, el artículo 5 inciso final, condiciona el uso de "los datos personales para los fines que motivaron la transmisión." En consecuencia, podemos observar que no queda regulada la proporcionalidad entre recopilación y tratamiento, sino que sólo entre transmisión y tratamiento.

Resulta indispensable llegar a aplicar este principio en nuestro país, puesto que en la mayor parte de los casos no se justifica que las empresas recolecten, procesen y vendan información de carácter personal, más allá de sus necesidades y de sus fines sociales.[19]

El *principio de transparencia* se encuentra recogido por la legislación chilena. En el artículo 4, el deber de informar se encuentra vinculado al consentimiento que presta el titular de los datos para autorizar el tratamiento de los mismos. Es así como, "la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público." Por otra parte, tratándose de la

[16] Este problema se vería atenuado de aprobarse un proyecto de ley se encuentra en trámite y que modifica precisamente la definición en comento (Boletín 3796-07).

[17] Herrera Bravo, Rodolfo, ***"Análisis de la Ley Chilena nº 19.628, sobre Protección de la Vida Privada, de 28 de agosto de 1999"***, p. 16, http://www.adi.cl/pdf/19628.pdf

[18] Ley 19.628, artículo 12 incisos 2° y 3°, respectivamente, en relación al artículo 6.

La misma ley (art. 2, letra d) entrega una definición de lo que ha de entenderse por "*dato caduco*": *"el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna."*

[19] Siguiendo y ampliando las ideas de Jaramillo Castro, Oscar, ***"La pérdida de la privacidad en internet"***, Textos de Docencia Universitaria, Universidad Diego Portales, Santiago de Chile, 2003, p. 110.

recolección de datos personales que se realiza a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, se deberá informar "del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información."[20]

La obligación de informar a las personas, se encuentra innecesariamente restringida, en cuanto a que el objeto de dicha obligación queda circunscrito únicamente al carácter obligatorio o facultativo de las respuestas y al propósito de la recolección o almacenamiento de los datos. Por consiguiente, no se comprenden los "elementos necesarios para garantizar un trato leal". Pensamos que la consagración de este principio resulta insuficiente, puesto que en primer lugar la obligación de informar debería aplicarse siempre que se recaben datos personales, en forma previa a la recolección de los datos. En segundo término, pareciera lógico ampliar el objeto de la obligación. Así debería comunicarse a la persona además, el propósito de cualquier operación de tratamiento de datos (no sólo recolección y almacenamiento), "los derechos que le reconoce la Ley y la individualización del responsable del registro [y del tratamiento] ante el cual ejercitarlos."[21]

Al tratar este deber de informar es importante diferenciarlo del derecho de acceso o a exigir información[22], puesto que en el primer caso el impulso de acción recae sobre el responsable de registro y tratamiento, asumiendo el titular de los datos una actitud de pasividad, mientras que en el segundo, se invierten los roles.

En lo que se refiere al *principio de seguridad,* éste sólo aparece en forma muy incipiente en la legislación chilena. Existe una norma relativa a la obligación de guardar secreto que afecta a "las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados" (art. 7). Asimismo, se le impone al responsable de las bases, en forma muy general, la obligación de cuidado de los datos personales, debiendo responder ante daños (art. 11).

Estas disposiciones son claramente insuficientes y no se adecuan a los avances tecnológicos de nuestros tiempos. En este sentido, conviene tener presente que el desarrollo tecnológico trae consigo tanto nuevos riesgos y peligros para la seguridad de los datos, como también herramientas y mecanismos para prevenir riesgos y mejorar la protección de los mismos. En suma, el panorama del tratamiento de la información evoluciona en forma radical y constante. Si bien resulta conveniente que el legislador enfrente dichos avances con criterios que promuevan la neutralidad tecnológica, nos parece absolutamente inapropiado no establecer claramente la obligación de adoptar medidas técnicas y organizativas adecuadas que garanticen "la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado."[23]

Los *Derechos de acceso, rectificación y oposición* tienen cabida en Chile. A los primeros dos de estos derechos ya hemos hecho alusión con anterioridad. Esta materia se encuentra reglamentada en el Título II "De los derechos de los titulares de datos".

El derecho de acceso, denominado por la ley "derecho a la información", se enuncia en el inciso 1° del artículo 12, cuando señala: *"Toda persona tiene derecho a exigir a quien sea*

[20] Artículo 3 de la Ley 19.628.

[21] Herrera Bravo, Rodolfo, *"Análisis de la Ley Chilena nº 19.628, sobre Protección de la Vida Privada, de 28 de agosto de 1999"*, ob. cit., pág. 21.

[22] El derecho de acceso o a exigir información se encuentra previsto en el artículo 12 y sgtes. de la Ley 19.628.

[23] Cita que corresponde al artículo 9 de la ley argentina sobre Protección de Datos Personales (Ley 25.326 de 4 de octubre de 2000), y que puede considerarse adecuada para cumplir con el principio en comento.

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."

La doctrina nacional ha criticado que se haya limitado la información sobre las trasmisiones de datos, restringiéndola innecesariamente al agregar la disposición transcrita la palabra "regularmente". Con ello, el responsable de una base de datos queda exento de informar acerca de los destinatarios ocasionales de los datos.[24] Agrava esta exclusión, el hecho de que las transmisiones ocasionales serán la regla, mientras que los destinatarios regulares serán muy pocos.

El derecho de rectificación, conocido legalmente como "derecho a modificación" se franquea al titular de los datos en los casos en que se acredite la falta de calidad de los datos personales, específicamente en los casos en que éstos "sean erróneos, inexactos, equívocos o incompletos."[25]

Conjuntamente con estos dos derechos, el artículo 12 se refiere al derecho de cancelación o de eliminación de datos[26], que procede en el evento que el almacenamiento de los datos "carezca de fundamento legal o cuando estuvieren caducos" o 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" (inc. 3° y 4° del art. 12). En este último caso, pudiera también ejercerse un derecho de bloqueo, que equivale a una "suspensión temporal de cualquier operación de tratamiento de los datos almacenados" (letra b del art. 2 de la ley). En este punto, "lo cierto es que, en la práctica, el bloqueo de datos se traduce en la imposibilidad de comunicar el dato bloqueado a terceros".[27]

En relación a estos tres derechos surge el derecho a obtener copia gratuita de los registros respectivos. Los pormenores de dichos derechos se encuentran desarrollados en los últimos incisos del artículo 12, así como en las disposiciones siguientes.

Podemos relacionar las normas de este título con el artículo 6, que establece la eliminación, modificación o bloqueo "de oficio" de los datos por parte del responsable del banco de datos personales, en caso de darse los supuestos descritos en el texto legal.

Los cuatro derechos descritos – información, modificación, eliminación y bloqueo – son limitados en cuanto a su ejercicio por el artículo 15 de la ley, en los siguientes casos:

- cuando impiden o entorpezcan el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido,
- cuando afecten el derecho de reserva o secreto establecido en disposiciones legales o reglamentarias, y
- cuando afecten la seguridad de la Nación o el interés nacional.

Además, no podrán ejercerse los derechos de modificación, eliminación y bloqueo de datos personales almacenados por mandato legal, a menos que exista autorización legal. Estimamos justificados estas cuatro excepciones, tanto en cuanto a su existencia como su envergadura.

[24] En este sentido: Herrera Bravo, Rodolfo, *"Análisis de la Ley Chilena nº 19.628, sobre Protección de la Vida Privada, de 28 de agosto de 1999"*, ob. cit., pág. 20.

[25] Artículo 12, inciso 2° de la Ley 19.628. En relación a ello, el artículo 2 letra j), define "*modificación de datos*", como "todo cambio en el contenido de los datos almacenados en registros o bancos de datos".

[26] *Eliminación o cancelación de datos*, es "la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello." (art. 2 letra h)

[27] Jervis Ortiz, Paula, *"Derechos del Titular de Datos y Habeas Data en la Ley 19.628"*, en "Revista Chilena de Derecho Informático", Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile, (2): 24, Mayo 2003.

Por último, encontramos que la normativa chilena también contempla un derecho de oposición; contrastando éste, sin embargo, con el buen tratamiento dado a los derechos hasta aquí descritos.

El artículo 3 en su inciso final, asegura al titular el derecho de "oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión." Consideramos en primer término criticable la ubicación de la norma dentro del Título I que contiene disposiciones generales. Por lógica, correspondería insertar este derecho dentro del Título II que precisamente se refiere a los derechos de los titulares. Enseguida, si comparamos el precepto referido con el artículo 14 de la Directiva Europea, podemos apreciar que en el caso chileno no existe una oposición preventiva, tal como la prevé el apartado 2° del referido artículo 14. Asimismo, destaca en la norma europea la amplitud de aplicación; restringiéndose en nuestro país el ejercicio del derecho a los casos relacionados con el marketing.

En lo referente al último principio – *restricciones respecto a transferencias sucesivas a otros terceros países* – éste simplemente se encuentra inexistente en Chile.[28] Evidentemente la carencia de normas sobre este principio demuestra un atraso grave de nuestra legislación sobre protección de datos, pero no es más que una consecuencia de las deficiencias generalizadas. Si la protección de los datos dentro las fronteras exhibe graves faltas, con mayor razón será en este campo.

3.1.2. *Principios específicos consagrados por la Legislación Chilena*

Estos principios adicionales tienen cabida sólo respecto de algunos tipos específicos de tratamiento de datos y, según el documento de trabajo del Grupo del Artículo 29, son los siguientes:

"1) Datos sensibles - cuando se trate de categorías de datos "sensibles" (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) Mercadotecnia directa - en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) Decisión individual automatizada - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona." [29]

Desarrollaremos a continuación cada uno de estos principios en cuanto a su aplicación en Chile.

El primero de ellos – datos sensibles – se encuentra contemplado en Chile bajo esta mis-

[28] La única norma que alude tangencialmente a este principio, pudiera ser el inciso final del artículo 5 que restringe su aplicación *"cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes."*

[29] Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, *"Working Paper 12"*, ob. cit.

ma denominación.[30] Se encuentra definido en términos bastante amplios, por el artículo 2° (letra g) como *"aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."*

La regla general es que este tipo de datos no puede ser objeto de tratamiento. La ley sólo admite tres excepciones taxativas:

1.- cuando la ley lo autorice,
2.- cuando exista consentimiento del titular, o
3.- cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.[31]

La regla general enunciada se ajusta a la Directiva Europea. Sin embargo, la ley guarda silencio en lo que respecta a las características del consentimiento del titular. Aplicando el argumento de la no distinción, sería suficiente que el titular consienta tácitamente[32]; ni siquiera se requeriría que fuese previo al tratamiento mismo. En lo relativo a las demás excepciones, éstas tampoco se encuentran muy especificadas.

Por otra parte, resulta curioso comparar el artículo 10 sobre el tratamiento de datos sensibles, con el artículo 4 sobre el tratamiento de datos personales en general. Se advierte que los dos casos en que la ley admite este último tratamiento – cuando la ley 19.628 u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello – son idénticas a los antes enumerados.

Finalmente, cabe hacer presente que actualmente se encuentra en trámite un proyecto de ley que modificaría la ley 19.628, en lo relativo al concepto de datos sensibles y otorgándole una reglamentación orgánica propia (Boletín 3796-07).

El segundo principio adicional, referido a la *mercadotecnia o marketing directo*, se encuentra regulado por el artículo 3 de la Ley 19.628, disposición a la que ya hemos hecho mención en diversas oportunidades anteriores.

Reiteramos aquí que dicha norma nos parece insuficiente en cuanto a su alcance, puesto que sólo se aplica tratándose de datos personales cuya recolección se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes. Esto nos parece criticable, por dos razones. Por un lado, se regula sólo la recolección de datos, y no las otras operaciones de tratamiento de datos. Por el otro, lo relevante para aplicar una norma reguladora del marketing directo, no es la forma de recopilación de los datos, sino que más bien los fines a los cuales se destinarán los datos personales. Así, en caso de que los datos se utilicen o se recaben con fines comerciales, promocionales o publicitarios, debería aplicarse una norma de estas características.

Por último, el *principio sobre la decisión individual automatizada* no se adopta realmente por la ley chilena de protección de datos. En forma vaga, toca el tema el artículo 5, ya que obliga al responsable de una base de datos que desea implementar un procedimiento automatizado de transmisión de datos, a resguardar los derechos de los titulares y al mismo tiempo a garantizar que la transmisión guarde relación con las tareas y finalidades de los organismos participantes. La misma disposición excluye su aplicación en los siguientes casos:

[30] En el derecho comparado suele hablarse de "dato especialmente protegido".
[31] Artículo 10 de la Ley 19.628.
[32] Por otro lado, con ayuda del artículo 4 pudiera concluirse por analogía que el consentimiento debe constar por escrito.

- cuando se trate de datos personales accesibles al público en general, y
- cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de tratados y convenios vigentes.

En suma, la ley chilena no contempla en forma expresa este principio. Si bien hay reglas generales acerca de la transferencia automatizada de datos, éstas no hacen mención si se involucran o no decisiones individuales automatizadas. En todo caso, sí se contemplan instancias protectoras del interés legítimo de los titulares de datos.

3.2. *Sistema de Aplicación Eficaz de la Legislación Chilena*

Según el documento de trabajo de 1998, para poder evaluar el carácter adecuado de la protección ofrecida por un determinado país, "es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados."

En este sentido, se precisan tres objetivos de un sistema de protección de datos:

"1) Ofrecer un nivel satisfactorio de cumplimiento de las normas. Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones." [33]

Revisaremos entonces, los mecanismos de procedimiento y de aplicación que ofrece el sistema chileno de protección de datos, en base a estos objetivos.

1) Nivel satisfactorio de cumplimiento de las normas:
En general hay que remarcar que nuestra ley sobre protección de la vida privada no ha permeado en profundidad en la conciencia de la opinión pública. Pese a que ya han pasado más de seis años desde la promulgación de la ley, existen aún amplios sectores de la población que ignoran los derechos y obligaciones contenidas en ella.

En lo que atañe a la existencia de sanciones efectivas y disuasorias, cabe mencionar que todas las sanciones que se impondrán en esta materia, tendrán carácter judicial, toda vez que no existe instancia administrativa alguna para ventilar asuntos de esta naturaleza.

[33] Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, *"Working Paper 12"*, ob. cit.

Dos son las acciones judiciales que ofrece la Ley 19.628 al titular de los datos, y las que abren la posibilidad de imponer sanciones. En primer lugar, como consecuencia de un procedimiento de "habeas data", el juez podrá establecer en la sentencia que acoge la reclamación, multas que van en una escala de una a cincuenta Unidades Tributarias Mensuales, según la gravedad de la infracción. Se consideran entre las infracciones más graves, aquellas que consisten en la negativa de eliminar o modificar datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, y cuya inclusión en el registro ya no se justifica (art. 16 incisos finales y art. 19 inciso final; esta última disposición en su versión modificada por la Ley 19.812).

En segundo término, el título V conformado por un artículo único, expresa que el "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." La acción de indemnización de perjuicios podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción. Concluye la disposición afirmando que "el monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos."[34]

Evidentemente, la circunstancia de que la ley chilena no haya implementado instancias administrativas para reclamar de las infracciones legales, se ha transformado en una de las deficiencias mayores del sistema. Lo anterior no es sino la consecuencia natural y lógica del hecho de que tampoco existe una autoridad de control. Los tribunales de justicia son los únicos llamados a ejercer un control de legalidad de carácter posteriori.

En consecuencia, Chile carece de sistemas de verificación directa por autoridades independientes. Si bien la ley instaura un registro de los bancos de datos personales a cargo de organismos públicos, que es llevado por el Servicio de Registro Civil e Identificación[35], a esta repartición de ningún modo le compete ejercer facultades fiscalizadoras, sino que una actividad de mera gestión registral. Cabe recordar que el Reglamento de la Ley 19.628, aprobado el año 2000 regula los pormenores del Registro de Banco de Datos Personales a cargo de los organismos públicos.

2) Apoyo y asistencia a los interesados en el ejercicio de sus derechos. Consecuente con lo anteriormente enunciado, podemos sostener que este factor tampoco se da en Chile, toda vez que el interesado sólo tiene la posibilidad de recurrir a instancias judiciales, engorrosas para el lego y sujetas a las formalidades procesales habituales. La representación judicial obligatoria que implica asumir costos financieros en forma anticipada y la lentitud común e inherente al sistema son un desincentivo potente a la hora de hacer valer sus derechos en materia de protección de datos personales. Por consiguiente, no existe en nuestro país ningún mecanismo institucional que permita investigar las denuncias de forma independiente y eficiente.

3) Vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas. De acuerdo a lo que ya hemos visto, nuestra ley contempla el recurso judicial de habeas data y las correspondientes sanciones e indemnizaciones. Veremos con mayor detalle este recurso común a las legislaciones latinoamericanas.

Sin perjuicio de la existencia de la modalidad preventiva del habeas data, que opera al ejercer el derecho de acceso, rectificación, cancelación o bloqueo directamente ante el responsable del banco de datos, aquí nos centraremos en la acción de habeas data que puede interponer judicialmente el titular de datos como una forma de control a posteriori y que se origina a partir de un incum-

[34] Artículo 23 de la Ley 19.628.
[35] Artículo 22 de la Ley 19.628.

plimiento de la legislación sobre protección de datos, teniendo por objeto obtener el acceso a sus datos personales y según el caso, su rectificación, cancelación o bloqueo.[36]

Siguiendo a la autora Paula Jervis, podemos constatar las siguientes causales de procedencia de la acción de habeas data:

- "Si el responsable del registro o banco de datos no se pronunciare sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles. (art. 16 inc. 1°)
- Si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una causa distinta de la seguridad de la Nación o el interés nacional. (art. 16 inc. 1°)
- Si el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por motivos de la seguridad de la Nación o el interés nacional. (art. 16 inc. 3°)
- Con la modificación introducida por la Ley 19.812, también se puede reclamar a través de este procedimiento por infracción a los artículos 17 y 18 de la Ley 19.628, que regulan la forma y los plazos en que pueden comunicarse a terceros por los responsables de los registros o bancos de datos de carácter económico, financiero, bancario o comercial. (art. 16 inc. 5°)
- Infracciones no contempladas en los artículos 16 y 19. (art. 23 inc. 2°)"[37]

En lo relativo al procedimiento de tramitación de la acción de habeas data nos remitimos a las disposiciones legales pertinentes (arts. 16 y 23), y respecto de las sanciones y reparaciones a lo señalado con anterioridad.

Fuera del habeas data, se encuentra a disposición del interesado otra acción de general aplicación: el recurso de protección; puede definírselo como una acción judicial que la Constitución chilena franquea a la persona afectada por una acción u omisión ilegal o arbitraria que le cause una privación, perturbación o amenaza en el legítimo ejercicio de un derecho fundamental. Por lo tanto, en caso de vulnerarse el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia, o la garantía constitucional de la inviolabilidad del hogar y de toda forma de comunicación privada, el interesado en restablecer el imperio del derecho podrá recurrir a través de esta acción rápida y eficaz a las instancias judiciales correspondientes.

En la práctica, los abogados ejercen con mayor preferencia la acción constitucional de protección, dejando de lado la acción del habeas data. Ello se debe fundamentalmente a que la primera es mucho más conocida – nació junto a la Constitución del año 1980 – y de aplicación mucho más extensiva, lo cual cobra importancia en los casos en que sean varias las garantías constitucionales transgredidas.

4. RESULTADO DE LA EVALUACIÓN Y CONCLUSIONES

Para llevar a cabo la presente evaluación del sistema de protección de datos en Chile, se han tomado en cuenta los diversos cuerpos normativos sobre el tema, así como jurisprudencia emanada de los tribunales superiores de justicia.

Asimismo, se han considerado los siguientes proyectos de ley que actualmente se encuentran en trámite en el Congreso Nacional:

[36] El habeas data preventivo o solicitud de habeas data se reglamenta en los artículos 12 al 15, mientras que la acción de habeas data o habeas data correctivo se encuentra consagrado en el artículo 16 de la Ley 19.628.

[37] Jervis Ortiz, Paula, *"Derechos del Titular de Datos y Habeas Data en la Ley 19.628"*, ob. cit., 27-28.

- Proyecto que amplía beneficios de ley sobre protección de la vida privada, en lo relativo a informes comerciales, a las personas jurídicas comprendidas en el artículo 545 del Código Civil (boletín 2474-07).
- Proyecto que modifica la ley 19.628, sobre protección de datos de carácter personal para introducir el concepto de uso indebido o abusivo de datos (boletín 3095-07).
- Proyecto que modifica la ley sobre protección de datos personales estableciendo sobre el uso de bases de datos en los correos electrónicos (boletín 3185-19).
- Proyecto que modifica la ley 19.628, con el fin de evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada (boletín 3796-07).

De estos proyectos naturalmente atraen la atención aquellos que pretenden otorgar cabida a las personas jurídicas como titulares de datos; ello debido a que en el derecho comparado son excepcionales las legislaciones que así lo prevén.

Otro tema muy actual es el tratamiento de los correos electrónicos no deseados, también llamado "spam". Si bien actualmente hay una disposición aislada en la ley de protección al consumidor sobre el tema, el proyecto en comento propone derogar dicho artículo y regularlo orgánicamente en la Ley 19.628.

Sin embargo, constatamos que pese a la tramitación de todos estos proyectos de ley, no se vislumbra una implementación cercana de los cambios necesarios en la materia objeto del presente trabajo. Creemos haber expuesto las numerosas falencias de la actual legislación de protección de datos, tanto en materia de principios como en las herramientas que aseguran el cumplimiento efectivo de las normas.

Dado lo anterior, concluimos que Chile no garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 de la 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.

Indudablemente existe premura en ponerse a nivel de legislaciones avanzadas en la materia, puesto que la protección de datos tal como la concebimos hoy en Chile, se convertirá en un freno para el desarrollo económico, social y cultural del país. Particularmente, la incidencia comercial-económica debería llamar la atención a las autoridades públicas, y motivar la proposición de una revisión generalizada de la ley existente, a fin de poner nuestra legislación a la altura de las europeas.

Evidentemente la piedra angular en dicha revisión general estará constituida por la decisión de implementar una autoridad independiente de control, y abrir con ello la puerta a instancias administrativas de cumplimiento efectivo y eficiente de la legislación. Ello iría de la mano con la educación de la opinión pública, partiendo de la base de que el dato personal es de propiedad del titular.

En este sentido, la creación de una verdadera conciencia con respecto a la protección de datos, causaría un completo replanteamiento de las transacciones comerciales en el país. Las siguientes frases, con las cuales concluimos, son reveladoras al respecto:

> *"Toda persona tiene un poder de disposición sobre sus datos, de controlar qué se hace con ellos. Cada uno es propietario de sus datos, que nunca pertenecen al titular del fichero. En este sentido, cada ciudadano debe ser el garante de su propio derecho, del uso que se hace de sus datos."* [38]

[38] PIÑAR MAÑAS, José Luis, "El derecho fundamental a la Protección de Datos de Carácter Personal", conferencia dictada en Curso de Verano "Presente y Futuro de la Protección de Datos Personales", organizado por Agencia Española de Protección de Datos, 20 de julio de 2004.