

# DOCTRINA CONSTITUCIONAL Y ADMINISTRATIVA

## LA LEY CHILENA DE PROTECCION DE LA VIDA PRIVADA

Por:  
Libardo Orlando Riascos Gómez  
Doctor en Derecho  
[Lriascos@udenar.edu.co](mailto:Lriascos@udenar.edu.co)  
2008

---

### ANÁLISIS DE LA LEY CHILENA Nº 19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA, DE 28 DE AGOSTO DE 1999 RODOLFO HERRERA BRAVO *Abogado*

1. [Introducción](#);
2. [La vida privada y la protección de datos personales en Chile, antes de la Ley Nº 19.628](#);
3. [La protección de datos personales, según la Ley Nº 19.628](#):  
Estructura de la Ley;  
Definiciones legales;  
Disposiciones generales relativas al ámbito de aplicación de la Ley;  
Derechos reconocidos por la Ley;  
La utilización o tratamiento de datos personales;
4. [Reflexiones finales](#);
5. [Bibliografía](#);
6. [Anexo 1](#): Ley Nº 19.628; LEY NUM. 19.628 SOBRE PROTECCION DE LA VIDA PRIVADA Diario Oficial de 28/8/99
7. [Anexo 2](#): Decreto Nº 779/2000, del Ministerio de Justicia. APRUEBA REGLAMENTO DEL REGISTRO DE BANCOS DE DATOS PERSONALES A CARGO DE ORGANISMOS PUBLICOS. Santiago, 24 de agosto de 2000

---

## 1. INTRODUCCIÓN

Chile ha sido uno de los países pioneros en Latinoamérica en abordar diversas problemáticas que suscitan las tecnologías de la información en la vida cotidiana. Tal es el caso, por ejemplo, de las modificaciones experimentadas por la Ley Nº 17.336, sobre Propiedad Intelectual, en 1985 y 1990 con el objeto de incorporar dentro de las obras especialmente protegidas a los programas computacionales; o al tipificar en 1993 ciertos delitos relacionados con la informática, en la Ley Nº 19.223; o en materia de protección de datos, gracias a la sanción en 1999 de la Ley Nº 19.628, sobre Protección de la Vida Privada.

Sin embargo, lo anterior no ha impedido que tales cuerpos normativos sean objeto de críticas desde diversos sectores, al considerar que dichas legislaciones son insuficientes o inapropiadas para abordar esos fenómenos. En el caso que nos ocupa –la Ley Nº 19.628–, trataremos de demostrar que la problemática de la protección de datos personales no es un tema desarrollado correctamente por legislador chileno, lo que amerita importantes modificaciones legales y desarrollos reglamentarios.

Se trata de un texto que ha sufrido una modificación sustancial en relación con el proyecto original presentado en el Senado en 1993, el cual no tuvo en vista convertirse en una ley de protección de datos, sino sólo perseguía aportar algunos instrumentos específicos que permitieran a las personas una efectiva defensa de sus vidas privadas ante eventuales atropellos o amenazas de que pudieran ser objeto en el ejercicio de este derecho, como ocurre con la Ley Orgánica Nº 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad personal y familiar y a la Propia Imagen, de España. Además, la ley de protección de datos se aparta de la estructura que suelen tener las respectivas legislaciones de otros países, y de los instrumentos internacionales existentes, sobre cuya base se supone ha sido creada.

El trabajo se limita a analizar el texto sancionado y vigente, a la luz de los debates parlamentarios y del derecho comparado que le sirvió de fuente. No entramos en detalle sobre la historia de su establecimiento ni en opiniones doctrinales, ya que, a nuestro juicio, Chile aún carece de una doctrina suficientemente clara en la cual apoyarse. Está dividido en dos partes: la primera, sobre la situación previa a la Ley Nº 19.628, pretende explicar los motivos de tan larga y cambiante tramitación –6 años y, a lo menos, tres proyectos

distintos-; y la segunda, que analiza el texto en vigor estructurado sobre la base de tres ideas principales, las disposiciones generales, los derechos que reconoce y la regulación que da al tratamiento de los datos.

En definitiva, este estudio pretende presentar brevemente la situación chilena sobre protección de datos a partir de la ley que directamente trata la materia, poniendo de manifiesto algunas de sus insuficiencias, pero sin agotar su análisis, el cual será fruto de próximos trabajos específicos a realizar en Chile con el objeto de educar jurídicamente al respecto, y, si es posible, crear un debate destinado a mejorar el intento que concretó el legislador en la Ley N° 19.628.

## **2. LA VIDA PRIVADA Y LA PROTECCIÓN DE DATOS PERSONALES EN CHILE, ANTES DE LA LEY N° 19.628**

Como bien señalaba la moción parlamentaria presentada en el Senado el 5 de enero de 1993, con la iniciativa de un proyecto de ley sobre protección de la vida privada se pretendía llenar un vacío manifiesto en el ordenamiento jurídico chileno. Reconocía la existencia de numerosas disposiciones dispersas en el ámbito civil, penal, mercantil, tributario o procesal que abordaban – y aún lo hacen- aspectos concretos del derecho fundamental a la vida privada o intimidad, sin la presencia de ningún texto legal que desarrolle el precepto constitucional del artículo 19 N° 4 de la Carta Fundamental, según el cual *“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 de su familia”* 1.

El proyecto del Senado reconocía la necesidad de desarrollo para ese derecho constitucional, aun cuando en la propia moción se mostraba a favor de un posterior texto refundido, coordinado y sistematizado, como *“una suerte de Código o Estatuto Jurídico de la Privacidad”* 2 que resolviera la dispersión normativa a que nos hemos referido. La principal fuente en que se apoyaba era la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que regula en España esos derechos fundamentales contenidos en el artículo 18.1 de la Constitución española. Por lo tanto, la finalidad de este proyecto era, simplemente, aportar algunos instrumentos específicos que permitiesen a las personas una efectiva protección civil de la vida privada ante eventuales atropellos o amenazas, calificados como intromisiones ilegítimas. Sin embargo, desde un principio se mostró como una Ley insuficiente al pretender, expresamente y de forma jurídicamente discutible, que sea la doctrina –que carece de fuerza vinculante- y la jurisprudencia –que tiene una función interpretativa con un ámbito restringido al caso concreto sometido a su decisión-, en vez del legislador, quienes fijen los límites de este derecho, su contenido, fundamentos y naturaleza jurídica.

De lo anterior, también se concluye que la protección de datos personales como garantía instrumental de los derechos fundamentales, entre otros, del derecho a la intimidad, no fue la motivación central del proyecto de ley, aunque en el Título II del texto presentado en el Senado se abordaran algunos principios básicos sobre el tema, circunscritos al tratamiento automatizado de datos nominativos. En efecto, la propia moción expresaba: *“nuestro proyecto apenas sienta algunas directrices mínimas que requieren de un necesario complemento mediante una Ley específica cuya promulgación no debe dilatarse más allá del tiempo que requiera un estudio acabado y minucioso”* 3.

El Título II del proyecto del Senado, denominado “De la protección de datos”, se basa en la Ley N° 78-17, de 6 de enero de 1978, sobre informática, ficheros y libertades, de Francia y la Ley N° 48, de 9 de junio de 1978, sobre registros de datos personales, de Noruega -ambas anteriores al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal-; además, de la Ley de 12 de junio de 1984, sobre protección de datos, de Gran Bretaña; y de los artículos 18.4 de la Constitución española y 35 de la Constitución portuguesa.

En términos generales, comenzaba declarando que la informática 4 debía estar al servicio de las personas y que su desarrollo debía realizarse respetando siempre el derecho a la vida privada. Por ello, nadie podría utilizar la informática para el procesamiento de datos personales sin consentimiento de su titular, salvo excepciones legales. Además, ya esbozaba la idea de ofrecer una regulación diferente a ciertos datos calificados por la doctrina como “sensibles”. Agregaba el deber de tomar precauciones para preservar la seguridad de las informaciones y reconocía al titular el derecho de acceder a sus antecedentes personales para conocer la fuente a la que se recurrió para obtenerlos, el uso que se les esté otorgando y los destinatarios de esas informaciones, junto con la facultad para exigir que sean rectificadas, completadas, aclaradas, actualizados o suprimidos. Finalmente, otorgaba un derecho a ser indemnizado de los perjuicios causados por el uso de datos inexactos, incompletos, equívocos, atrasados o caducos.

Tras la discusión y aprobación del proyecto de ley en el Senado –primer trámite constitucional-, fue sometido al estudio de la Cámara de Diputados. En esa oportunidad el proyecto sufrió una modificación íntegra en la Comisión de Constitución, Legislación y Justicia de la Cámara, transformando un muy general e incompleto proyecto de ley sobre protección civil de la vida privada -que pudo ser mejorado durante su tramitación-, en un insuficiente e impreciso proyecto de protección de datos personales, por considerar que este tema era desarrollado con mayor propiedad y profundidad. Es decir, al pasar al segundo trámite constitucional se comienza a discutir un texto completamente distinto al del Senado, con una finalidad y un ámbito también diverso, mucho más acotado.

Este nuevo texto, ahora exclusivamente sobre protección de datos personales, con algunas modificaciones realizadas en la Cámara de Diputados, fue presentado en 1998 al Senado, en tercer trámite constitucional. Sin embargo, como consecuencia de la renovación parlamentaria de ese año y, principalmente, porque la Cámara modificó el proyecto aprobado en primer trámite, se decidió enviar la iniciativa a la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, quien, en su informe, rechazó la iniciativa. Como consecuencia, el Senado hizo lo propio y se acordó la formación de una Comisión Mixta encargada de proponer el modo de resolver las divergencias suscitadas entre ambas Cámaras, surgiendo a partir de su informe el texto final de la Ley N° 19.628, sobre Protección de la Vida Privada, que comenzaremos a analizar.

### **3. LA PROTECCIÓN DE DATOS PERSONALES, SEGÚN LA LEY N° 19.628**

#### **3.1. Estructura de la Ley**

La Ley N° 19.628, publicada en el Diario Oficial de 28 de agosto de 1999, consta de un Título Preliminar, sobre Disposiciones Generales, como su ámbito de aplicación y un conjunto de definiciones legales; cinco Títulos: De la utilización de datos personales, De los derechos de los titulares de datos, De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, Del tratamiento de datos por los organismos públicos, y De la responsabilidad por las infracciones a esta Ley; y un Título Final que agrega una disposición al Código Sanitario. Además, contiene tres disposiciones transitorias. La primera fija dos períodos de vacancia legal: uno de sesenta días contados desde la publicación en el Diario Oficial, por el cual la Ley entró en vigencia en octubre de 1999; y otro de un año desde dicha publicación, para el artículo 22 que, como veremos, dispone la creación de un registro de bancos de datos personales a cargo de organismos públicos. Por su parte, la disposición transitoria segunda hace extensivos los derechos que confiere la Ley a los titulares de datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de este cuerpo legal. Y la tercera, amplía la vigencia del decreto supremo N° 950, de 1928, del Ministerio de Hacienda, que regula el Boletín de Informaciones Comerciales, en todo lo que no sea contrario a esta Ley.

#### **3.2. Definiciones legales**

Comenzaremos este análisis con una revisión de los conceptos que define el legislador para este cuerpo normativo, técnica apropiada para leyes sobre materias nuevas o muy técnicas, que ameritan una claridad conceptual que facilite la interpretación.

En relación con los sujetos que intervienen, se encuentra la figura del TITULAR DE LOS DATOS, es decir, *“la persona natural a la que se refieren los datos de carácter personal”* 5 que se someten al tratamiento regulado por esta Ley. Esto, además, significa, a *contrario sensu* y en relación con el concepto de dato personal a que nos referiremos, que las personas jurídicas no están protegidas por esta normativa al no ser titulares de datos.

Por otra parte, señala qué se entiende por RESPONSABLE DEL REGISTRO O BANCO DE DATOS, indicando que será *“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”* 6. En relación con la expresión “ORGANISMO PÚBLICO”, está acotada a *“las autoridades, órganos de Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado”* 7, 8.

Sin embargo, limitarse a señalar que el responsable es aquel a quien compete las decisiones relacionadas con el tratamiento es poco preciso, ya que en una persona jurídica pública o privada, el tipo de decisiones realmente significativas para los efectos de esta Ley, tales como las finalidades y usos del tratamiento o los medios y contenidos le corresponden normalmente a los directivos de la organización o del departamento en

que se encuentren las bases de datos, y no a los operadores directos de los sistemas de información, por ejemplo, quienes también toman decisiones al respecto, pero en un nivel inferior. La responsabilidad, por lo tanto, no puede ser la misma, por lo que se extraña para estos últimos una figura semejante a la del encargado del tratamiento 9 , quien trata los datos por cuenta del responsable. No obstante, creemos adecuado que la función de responsable la ocupe quien efectivamente tome las decisiones en último término, pudiendo corresponder o no con los más altos directivos. Por último, al considerar como responsable del tratamiento a una persona jurídica, y no sólo a una persona natural, dificulta la aplicación práctica de responsabilidades, en particular las penales y administrativas.

La regulación que ofrece la Ley está dirigida al TRATAMIENTO DE DATOS, un concepto genérico que comprende acciones diversas destinadas a objetivos tan dispares, tales como la recogida de datos, su cesión a terceros o su eliminación, y que se define como *“cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma”* 10 . Cabe destacar el carácter técnico de dichas operaciones y procedimientos, y la posibilidad que se efectúen manual o automatizadamente, idea que se reitera con la definición de REGISTRO O BANCO DE DATOS, entendida como *“el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos”* 11 . Dentro de las operaciones y procedimientos que se consideran tratamiento de datos, la Ley ha definido expresamente algunos. En primer lugar, entiende por ALMACENAMIENTO DE DATOS a *“la conservación o custodia de datos en un registro o banco de datos”* 12 , operación que, a nuestro juicio, lleva implícita para el responsable del registro una obligación de seguridad de dichos datos, ya que conservar y custodiar implican el guardar con cuidado y vigilancia una cosa. Sobre la MODIFICACIÓN DE DATOS, es decir, *“todo cambio en el contenido de los datos almacenados en registros o bancos de datos”* 13 podemos advertir que, si bien no se refiere a cambios formales de los datos, las alteraciones estructurales de los registros en donde se encuentran almacenados pueden ser, en ocasiones, más peligrosas que los cambios de fondo, debido a la posibilidad de cruzar algunos datos para efectuar valoraciones de aspectos determinados de la personalidad del titular.

La COMUNICACIÓN O TRANSMISIÓN DE DATOS, corresponde a lo que también se denomina cesión en el derecho comparado, y consiste en *“dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas”* 14 . Resaltamos que la revelación de datos a terceros puede ser de cualquier forma, no sólo a través de algún soporte físico que haga susceptible de tratamiento a dichos datos por parte de terceros, por ejemplo, entregándolo en un certificado, enviándolo en formato digital por una red, o permitiendo su mera visualización.

En relación con el PROCEDIMIENTO DE DISOCIACIÓN DE DATOS, se refiere a *“todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable”* 15 , definido en términos casi idénticos a la Ley Orgánica 5/1992 sobre Regulación del tratamiento automatizado de los datos de carácter personal (en lo sucesivo, LORTAD), de España, derogada y sustituida por la Ley Orgánica 15/1999, de Protección de datos de carácter personal (en adelante, LOPD). Se trata de un procedimiento cuya complejidad variará en cada caso concreto. Por ejemplo, si se deben utilizar datos disociados sobre remuneraciones o sobre ausencias o atrasos laborales, el número de trabajadores será determinante, ya que si son muchos, la imposibilidad de asociar la información con un trabajador determinado puede lograrse simplemente eliminando su nombre, pero manteniendo otros datos como el tipo de cargo que ocupa. Sin embargo, si son pocos, es muy probable que se necesite un nivel mayor de disociación. Cabe agregar que producto del procedimiento de disociación se generan DATOS ESTADÍSTICOS, ya que se trata de un *“dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable”* 16 .

La figura del BLOQUEO DE DATOS, institución introducida por la legislación alemana de protección de datos, está definida como *“la suspensión temporal de cualquier operación de tratamiento de los datos almacenados”* 17 . El bloqueo, al sólo dejar irreconocible los datos, no debe ser considerada como una alternativa morigerada de la ELIMINACIÓN O CANCELACIÓN DE DATOS, entendida como *“la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello”* 18 . Más bien, el bloqueo debe ser una respuesta frente al riesgo que genera el proceso de cancelación o eliminación para datos de presumible interés histórico, para evitar así un borrado parcial de la historia.

La Ley también establece distintos tipos de datos personales lo que se justifica atendiendo a la estructura que presentan la generalidad de leyes de protección de datos. En ellas se distinguen tres clases que requieren distintos niveles de protección. Así, las disposiciones generales de estas leyes se les aplican a los llamados

“datos personales de protección ordinaria”; sin embargo, para otros deben ofrecer menos limitaciones al tratamiento –lo que no significa que sean datos inocuos-, constan normalmente en fuentes accesibles al público y se refieren a “datos de mera identificación”. Y por último, están los “datos sensibles”, que requieren una protección especial, mayor que la ordinaria, que en un principio se traduce en la prohibición de tratamiento.

En tal sentido, la Ley comienza definiendo DATOS DE CARÁCTER PERSONAL O DATOS PERSONALES como *“los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”* 19 . Como primer comentario debemos concordar esta definición con lo expresado precedentemente sobre el titular de los datos, y concluir que la información que se protege por esta normativa le concierne sólo a una persona natural, por cierto, único titular de vida privada o de intimidad, principal derecho fundamental a proteger que orientó al legislador desde los orígenes de la tramitación del proyecto. La exclusión de las personas jurídicas de esta protección es correcta, ya que en su caso existen otros principios en juego, como la transparencia de su gestión, y no el secreto de sus actividades. La información de las personas jurídicas no recibe un tratamiento igual al de las personas naturales y se la puede proteger con otras normas, como las de secreto comercial o industrial.

Una segunda observación se refiere al tipo de información que se considera dato personal. La interpretación correcta y hacia la cual están evolucionando las normativas internacionales, es a entender dentro de los datos personales no sólo a la información alfanumérica sobre un individuo, sino también aquella que ofrecen las imágenes grabadas por vídeo o las fotografías, o la voz de la persona. Creemos que esa extensión debe darse en este caso, sobre todo por definir al dato personal como “cualquier información”.

Por último, un tercer aspecto de esta definición que destacaremos es el sentido de la expresión “identificable”. Acudiendo a la Directiva 95/46, antes anotada, se entenderá identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Continuando con la distinción de los tipos de datos, la Ley define DATOS SENSIBLES entendiendo por tales a *“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”* 20 . Si bien, en términos generales concuerda con las nociones doctrinales escritas sobre la materia no sigue la técnica legislativa abordada por las normativas que tuvieron a la vista los legisladores durante la tramitación.

En efecto, el Convenio 108 del Consejo de Europa, al referirse en su artículo 6 a las “Categorías particulares de datos”, da una enumeración mucho más cerrada de datos sensibles, indicando que *“los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones [léase filosóficas o ideológicas], así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales”* 21 .

La Directiva 95/46 CE, por su parte, en el artículo 8 regula el “Tratamiento de categorías especiales de datos”, indicando que *“[...] Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. [...] El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional [...] Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos”* 22

En España, la LOPD, e incluso la derogada LORTAD, no definen los datos sensibles sino que se limitan a referirse de forma particular en el artículo 7 a ciertos datos especialmente protegidos, indicando que *“[...] Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias [...] Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente [...] Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes [...]”* 23 .

En Chile, el legislador, junto con definirlos dispone que no pueden ser objeto de tratamiento, salvo cuando la Ley lo autorice, el titular consienta en ello –no expresa mayores detalles, aunque remitiéndonos a otras normas, entendemos que de forma escrita-, o si son necesarios para determinar u otorgar beneficios de salud que correspondan a sus titulares 24.

El concepto que da la Ley nos parece muy amplio, por lo que normalmente será el juez quien tenga que interpretar en cada caso particular si el dato en cuestión es o no sensible y, por lo tanto, si su tratamiento está prohibido *a priori*, salvo en las excepciones que fija esta Ley. En tal sentido, la normativa sobre datos sensibles operará en muchos casos discutibles sólo una vez generado el conflicto jurídico, ya que la primera calificación la efectuará el responsable del registro, quien normalmente tendrá una pretensión diametralmente opuesta a la del titular del dato, ya que a aquél le interesará tratar dicha información con exigencias menores a las que se aplican a los datos sensibles.

Creemos que basar la regulación especial que deben recibir los datos sensibles en un concepto tan general, con una enumeración fijada a modo ejemplar 25, sin contener disposiciones específicas para los casos de datos sensibles comúnmente aceptados por el derecho comparado, puede derivar en que la Ley, con una estructura troncal centrada en disposiciones generales para los datos personales de protección ordinaria y normas especiales para los datos públicos de mera identificación y para los sensibles, termine vaciándose de contenido, en la medida en que en la práctica se tienda a asemejar el concepto de dato personal con el de dato personal sensible.

En otro orden de ideas, el legislador define el DATO CADUCO, aludiendo a un importante estado en que puede encontrarse, por las consecuencias que acarrea, según veremos más adelante. Indica que es *“el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna”* 26.

Finalmente, aunque la Ley no define los datos públicos de mera identificación, podemos entender por tales aquellos que se encuentran en FUENTES ACCESIBLES AL PÚBLICO, concepto que el legislador entiende como *“los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes”* 27.

Sin embargo, lamentamos que no se haya seguido a la legislación española en este punto, ya que la LOPD, junto con definir en su artículo 3, letra j), a las fuentes accesibles al público como *“aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación [...]”*, procede a tasarlas, manteniendo de este modo su carácter especial en relación con los datos personales de protección ordinaria. En efecto, en España son fuentes accesibles al público exclusivamente el censo promocional –aún no creado-, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales –sólo respecto de ciertos datos-, los Diarios y Boletines oficiales y los medios de comunicación.

En Chile, en cambio, existen algunas fuentes de acceso restringido por la ley en atención al carácter reservado o confidencial de los datos que contienen, como es el caso del secreto estadístico, tributario, bancario o el filiación política, o las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud 28. Sin embargo, lo normal es que no existan estas normas restrictivas, debiendo ser los jueces, nuevamente, quienes determinen en cada caso en particular si existe tal restricción o reserva para acceder a los datos en cuestión. En definitiva, nos parece un error los términos tan amplios de la definición, ya que no hay que olvidar que el régimen de los datos contenidos en las fuentes accesibles al público –al igual que como ocurre con los datos sensibles- debe ser especial y no la regla general.

### **3.3. Disposiciones generales relativas al ámbito de aplicación de la Ley**

De conformidad con el artículo 1 de la Ley, se sujetan a ella las operaciones y procedimientos técnicos sobre datos personales que constituyan un tratamiento de datos, automatizado o manual estructurado, realizados por organismos públicos o por particulares, sean personas naturales o jurídicas. Sin embargo, para que se les aplique esta Ley se requiere que tales datos personales no se encuentren aislados, sino que formen un conjunto organizado, es decir, un registro o banco de datos. Se excluye de esta normativa al tratamiento de datos personales que se efectúe en ejercicio de las libertades de emitir opinión y de informar, cuyo desarrollo le corresponde a otra ley de acuerdo al artículo 19 N° 12, de la Constitución Política 29. Podría estimarse acertado, si consideramos que dentro de las líneas que siguen las leyes de protección de datos está la búsqueda de equilibrio entre los distintos intereses en juego, entre ellos la libertad de información. Pero, la

exclusión absoluta de las empresas de comunicación social del ámbito aplicativo de la Ley de protección de datos, puede convertirse en un aumento de privilegios para la minoría que disponga de recursos para explotar la información. Lo más razonable habría sido prever un régimen especial para los registros o bancos de datos de las empresas de comunicación social, en vez de depender de otro cuerpo normativo. No nos detendremos en este punto, porque el análisis de esa legislación escapa a nuestro estudio.

### 3.4. Derechos reconocidos por la Ley

En primer término, el legislador concede a toda persona natural o jurídica la facultad para tratar datos de carácter personal, obviamente, siempre que lo haga en conformidad con esta Ley y para una finalidad permitida por el ordenamiento jurídico. Lo interesante de recalcar de esta disposición se refiere a la limitación que inmediatamente impone a este derecho: el tratamiento deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta Ley les reconoce 30 . Sin entrar en profundidad en el tema de las limitaciones haremos una observación, referida a la garantía constitucional del artículo 19 N° 26, en cuya virtud: *“La Constitución asegura a todas las personas: [...] la seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio”*. Esto significa que las injerencias que a partir de esta Ley sufran los derechos constitucionales de los titulares de datos, no pueden significar un desconocimiento del contenido esencial o núcleo irreductible de éstos, so pena de transformarse en limitaciones ilegítimas e inconstitucionales.

Por otra parte, dentro de las facultades que concede, reconoce un DERECHO DE ACCESO, en cuya virtud todo titular podrá exigir al responsable del registro de datos personales 31 , información sobre los datos relativos a su persona, su procedencia y destinatario, la finalidad del almacenamiento y la individualización de las personas u organismos a los cuales sus datos sean transmitidos regularmente. No encontramos justificación a la expresión “regularmente”, con la cual se restringe este derecho a ser informado únicamente sobre los destinatarios frecuentes de una comunicación y no respecto de una cesión puntual 32 . Por otra parte, el titular cuenta con un DERECHO DE RECTIFICACIÓN 33, que le permite exigir que se modifiquen aquellos datos suyos probadamente erróneos, inexactos, equívocos o incompletos. Ahora, si los datos almacenados carecen de fundamento legal o están caducos, o incluso cuando los haya proporcionado voluntariamente o se usen para comunicaciones comerciales y no desee seguir figurando en el registro respectivo, puede eliminarlos, salvo excepciones legales, gracias a un DERECHO DE CANCELACIÓN 34. Entendemos que la posibilidad de eliminar los datos proporcionados voluntariamente es la lógica consecuencia a una revocación del consentimiento otorgado para su tratamiento, revocación que debe manifestarse por escrito, y no puede tener efecto retroactivo 35 . El legislador no exige causa justificada para cancelar estos datos, lo cual puede resultar excesivo para quienes desarrollan legítima y lealmente su actividad de tratamiento de datos, recordemos que en este caso no se trata de datos caducos ni almacenados sin fundamento legal, sino únicamente existe una decisión del titular a revocar la autorización que entregó en su momento. Además, en el caso anterior y cuando los datos se usen para comunicaciones comerciales y no se desee seguir figurando en el registro respectivo, se ofrece la alternativa de bloquear los datos temporalmente 36 . Nos remitimos a lo señalado precedentemente sobre esta figura.

Este derecho a eliminar datos que se usen para comunicaciones comerciales debe entenderse en relación con el derecho que la Ley concede para oponerse a la utilización de los datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Para hacer posible el ejercicio de esta facultad, el legislador ha dispuesto que en toda recolección de datos personales realizada a través de encuestas, estudios de mercado o sondeos de opinión pública se debe informar -entendemos que previo a la recogida- del carácter obligatorio o facultativo de las respuestas y la finalidad para la cual se solicitan los datos. Sin embargo, estimamos insuficiente esa información, ya que también se debería advertir a la persona sobre los derechos que le reconoce la Ley y la individualización del responsable del registro ante al cual ejercitarlos 37.

El ejercicio de estos derechos de acceso, rectificación y cancelación –denominados por la Ley como derechos a exigir información, modificación o eliminación de datos, respectivamente- debe ser gratuito y, si el titular lo solicita personalmente, hay que acompañar una copia del registro alterado en la parte pertinente. Sin embargo, si se efectúan nuevas modificaciones o eliminaciones de datos, el titular puede obtener gratuitamente una copia del registro actualizado, siempre que hayan transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho 38.

Además, la solicitud del titular debe ser respondida por el responsable del registro dentro de dos días hábiles y, en caso de denegarla, este hecho debe fundarlo en razones de seguridad o interés nacional, ya que si no se pronuncia dentro de plazo o deniega por una causa distinta, el titular de los datos tiene derecho a recurrir

al juez de letras en lo civil correspondiente al domicilio del responsable solicitando amparo de sus derechos 39. Sin perjuicio de lo señalado sobre estos derechos del titular, la Ley impone, además, algunas obligaciones al responsable del registro que deben ser cumplidas de oficio. Es el caso de la cancelación de los datos cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado; su modificación cuando sean erróneos, inexactos, equívocos o incompletos; o su bloqueo cuando la exactitud de la información no pueda ser establecida o su vigencia sea dudosa 40. Por último, si los datos cancelados o modificados fueron comunicados previamente a terceros, el responsable debe avisarles a la brevedad este hecho. Esta obligación está incompleta, porque no se obliga a los cesionarios de los datos a realizar asimismo las correspondientes cancelaciones o rectificaciones 41.

No obstante todo lo dicho sobre los derechos de acceso, rectificación, cancelación o bloqueo, la Ley prohíbe su ejercicio cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público responsable del registro o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional. Además, cuando el tratamiento lo exige una ley, será ésta quien determine si es posible o no que el titular de los datos solicite su modificación, eliminación o bloqueo 42.

Por último, sin perjuicio del derecho a modificar, bloquear o eliminar los datos, la Ley concede al titular el derecho a que el responsable del registro le indemnice del daño patrimonial y moral causado por un tratamiento indebido de datos. El ejercicio de dicha acción se hará ante la jurisdicción ordinaria, bajo un procedimiento sumario, facultándose al juez para apreciar la prueba en conciencia y para establecer prudencialmente el monto de la indemnización, considerando las circunstancias del caso y la gravedad de los hechos 43.

### 3.5. La utilización o tratamiento de datos personales

La Ley ha optado por fijar en el artículo 4, una regla general sobre la utilización de datos personales, para luego regular excepciones. El legislador establece que sólo puede efectuarse el tratamiento bajo dos supuestos: cuando esta Ley u otras disposiciones de rango legal lo autoricen, o bien, cuando el titular de los datos da su consentimiento de forma expresa. El principio del consentimiento, pilar de las leyes de protección de datos del derecho extranjero, ha sido desarrollado de forma dubitativa, al extremo de convertirse, a nuestro juicio, en una débil declaración romántica que no ampara efectivamente al titular. Aunque la Ley disponga que el tratamiento de datos sólo podrá realizarse con el consentimiento expreso, e incluso por escrito, no exige que sea específico, por lo que nada obsta a que en la práctica se utilice deslealmente un modelo de cláusula de consentimiento que pueda esconder un alcance mayor al que, en un comienzo, motivaba al titular.

Además, apoya este principio en una insuficiente información previa. No basta con señalar que la persona que autoriza debe ser debidamente informada del propósito del almacenamiento y de su posible comunicación al público, si se desconocen los derechos que se pueden hacer valer y el nombre y domicilio del responsable del registro. Más aún, si la información acerca de eventuales comunicaciones a terceros luego no se refleja en la obligación de requerir nuevamente el consentimiento específico e inequívoco del titular, para poder realizarlas, se transforma en una simple "información de cortesía".

Sin perjuicio de lo anterior, hay que concluir que la regla general que establece la Ley es la necesidad de consentimiento escrito para proceder al tratamiento de datos personales. Pero como adelantamos precedentemente, el legislador contempla excepciones a dicha regla según las cuales la utilización de los datos no requiere autorización del titular. Ello ocurre en los siguientes casos:

- cuando los datos personales provengan o se recolecten de fuentes accesibles al público. En particular, cuando sean **datos personales de carácter económico**, financiero, bancario o comercial; cuando se contengan en listados relativos a una categoría de personas, pero limitados a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento; y cuando sean datos necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios;
- cuando el tratamiento lo realizan personas jurídicas privadas cumpliendo los siguientes requisitos copulativos: los datos tratados son para uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas; y se realiza con fines estadísticos, de tarificación u otros de beneficio general de aquéllos; y
- cuando el tratamiento lo efectúa un organismo público respecto de las materias de su competencia 44.

Ahora bien, en relación con la comunicación o cesión de los datos, el legislador incurre en una lamentable omisión al no regularla en términos generales, refiriéndose a ella a propósito de algunas situaciones específicas. Es decir, no hay una obligación general de requerir el consentimiento inequívoco y específico del titular para efectuar una comunicación a terceros, salvo excepciones, sino, por el contrario, la comunicación de datos exige únicamente una obligación de informar la posible ocurrencia de este hecho, al momento de recolectar los datos.

Uno de los casos en que la Ley se detiene sobre el tema de la comunicación es el artículo 5, que concede al responsable del registro la posibilidad de establecer un procedimiento automatizado de transmisión de datos, siempre que cautele los derechos de los titulares y la transmisión esté relacionada con las tareas y finalidades de los organismos participantes en ella. Se exige que la admisibilidad de todo requerimiento de datos personales mediante una red digital sea evaluada por el responsable del registro, el cual debe dejar constancia de la individualización del requirente, el motivo y la finalidad de la petición, y el tipo de datos que se transmiten. Además, el receptor de los datos sólo puede utilizarlos para los fines que motivaron la comunicación. No obstante, estas mínimas y razonables exigencias legales no son aplicables si los datos proceden de una fuente accesible al público o si el destinatario es una organización internacional a la cual se le envían en cumplimiento de tratados y convenios vigentes.

Otra de las situaciones referidas a la comunicación, a la que alude expresamente la Ley, atañe a los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias. Según el artículo 21, dichos organismos no podrán comunicar a terceros tales datos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, a menos que les sea solicitada por los tribunales de justicia u otros organismos públicos competentes.

Finalmente, la comunicación también es tratada en los artículos 17 a 19, con relación a los **datos personales de carácter económico**, financiero, bancario o comercial. En este caso –que, como vimos, constituye una excepción al principio del consentimiento–, los responsables de los registros pertinentes sólo podrán comunicar los datos personales que versen sobre obligaciones de carácter económico, financiero, bancario o comercial, si se encuentran en cualquiera de las siguientes hipótesis:

- cuando consten en letras de cambio y pagarés protestados;
- cuando consten en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa;
- cuando se trate del incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales;
- cuando sean otras obligaciones de dinero, determinadas por decreto supremo del Presidente de la República y sustentadas en instrumentos de pago o de crédito válidamente emitidos en los que conste el consentimiento del deudor y su fecha de vencimiento.

Sin embargo, dicha comunicación está limitada en el tiempo, bajo la figura que la doctrina denomina “derecho al olvido”. En ningún caso pueden comunicarse esos datos luego de transcurridos siete años desde que la respectiva obligación se hizo exigible, ni continuar revelándolos después de tres años desde que la obligación se ha extinguido por el pago u otro modo legal. Cabe advertir que mientras esté pendiente el plazo de tres años posterior al pago de la deuda o su extinción por otra vía, el titular no puede solicitar la modificación, eliminación o bloqueo de sus datos, y que el responsable del registro debe comunicarlos a los tribunales de justicia que lo requieran con motivo de juicios pendientes 45.

Una vez extinguida la obligación por el pago o por otro modo en que intervenga directamente el acreedor, por ejemplo, a través de la compensación o la novación, el responsable del registro de datos accesibles al público que en su oportunidad comunicó la situación de morosidad del deudor, debe ser avisado de tal hecho por el acreedor dentro de los siete días hábiles siguientes, para que actualice la información. El pago de tarifas que procedieran por este hecho, será de cargo del deudor, quien, además, podrá optar por liberar de esta obligación al acreedor y solicitar directamente la modificación del banco de datos.

Esta obligación de modificar los datos una vez extinguida la deuda para que así correspondan a la situación real del titular, también incumbe a quienes traten estos datos provenientes o recolectados de la fuente accesible al público que los almacene, tan pronto como el responsable de ésta le comunique el hecho, o

dentro de los tres días hábiles siguientes. Sin perjuicio de ello, hasta que actualicen la información deben mantener bloqueados los datos pertinentes 46 .

En otro orden de ideas, la Ley se refiere a los principios de finalidad y calidad de los datos, ampliamente reconocidos en las distintas normativas extranjeras sobre la materia. En efecto, dispone que los datos sean utilizados sólo para los fines para los cuales hubieren sido recogidos, salvo que provengan o se hayan recolectado de fuentes accesibles al público. No obstante, siempre la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos 47 Deteniéndonos brevemente en el principio de finalidad observamos que se desarrolla a lo largo de la Ley sin la fuerza suficiente, y ello no sólo porque las fuentes accesibles al público puedan ser numerosas en la práctica, sino más bien, porque no exige que la finalidad sea determinada y explícita, y porque, a nuestro juicio, 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.

Ya próximos a final de este trabajo, aludiremos a otro de los principios que recoge la Ley. Se trata del deber de secreto y custodia de los datos, por el cual quienes trabajan en el tratamiento de datos personales –no sólo el responsable del registro- deben guardar secreto de los mismos, salvo que provengan de fuentes accesibles al público, extendiéndose esta obligación incluso después de terminar sus actividades. Además, la Ley agrega que el responsable de los registros donde se almacenen datos personales debe cuidar de ellos con la debida diligencia, haciéndose responsable de los daños, lo que a nuestro juicio no es más que una declaración romántica carente de eficacia práctica en materia de seguridad de los datos, en la que se limita a repetir la regla general sobre responsabilidad civil, sin siquiera remitir a un desarrollo reglamentario.48.

Finalmente, es dable agregar unas observaciones sobre el registro a que se refiere el artículo 22. Dicha norma encarga al Servicio de Registro Civil e Identificación llevar un registro público de los bancos de datos personales a cargo de organismos públicos, en el cual ha de constar el fundamento jurídico de la existencia de cada banco de datos, su finalidad, los tipos de datos almacenados y la descripción del universo de personas que comprende 49 . Agrega la norma que 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 dentro de los quince días desde que se produzca.

Según la historia fidedigna del establecimiento de esta Ley, reflejada en el informe de la Comisión Mixta, se decidió encomendar esta función al Servicio de Registro Civil e Identificación, ya que su experiencia y su cobertura territorial lo convertían en el organismo más idóneo para realizarla y permitir a los particulares un fácil acceso a la información respectiva. Además, cabe advertir que no se incluyó el registro de los bancos de datos personales de carácter privado, por estimarse de una dificultad considerable el hacerlo, ya que se desconoce el número de ellos y sus características. Es más, frente a la intención de uno de los parlamentarios de crear también un registro de los bancos de datos personales que tienen particulares, las observaciones que se le hicieron indicaban que al dotar de tales atribuciones a un servicio público se incursionaría en el ámbito fiscalizador, planteando problemas relacionados con el rol del Estado, con la naturaleza registral propia del Servicio de Registro Civil e Identificación, incluso con dificultades de índole presupuestaria.

Sin embargo, también hay que reconocer que los legisladores admitieron que la Ley es sólo un primer paso en la materia y, específicamente, que este registro constituía un avance frente a la situación actual de inexistencia de ellos.

#### **4. Reflexiones finales**

Comenzábamos el trabajo indicando nuestra opinión sobre la Ley, según la cual creemos que el tema de la protección de datos personales no está desarrollado correctamente por el legislador chileno, lo que amerita importantes modificaciones legales y desarrollos reglamentarios. Con nuestro análisis hemos pretendido demostrarlo, eso sí, sin entrar en un estudio pormenorizado de la norma. No obstante, a modo de reflexión final, haremos hincapié en algunos aspectos.

Dado que las leyes de protección de datos del derecho extranjero tienden a diseñarse bajo una estructura común, es necesario establecer si la Ley N° 19.628 también se ciñe a ella. Estas legislaciones tratan de lograr un equilibrio entre los derechos fundamentales que suelen encontrarse en juego, por ejemplo, garantizando el respeto de la intimidad y otros derechos de los titulares de los datos, pero sin impedir

excesivamente la libertad de información, la libertad de empresa de quien efectúa el tratamiento, o la necesidad de información que requiere el Estado, sobre todo, social.

Además, el nivel de protección varía en atención al tipo de dato personal de que se trate. Si bien ningún dato personal es inocuo, no todos requieren la misma protección. Así, la regla general son los datos de protección ordinaria, aunque es necesario contemplar situaciones especiales en que las normas deben ser morigeradas ante datos de mera identificación, o aumentadas, prohibiendo el tratamiento de datos sensibles que no cuente con autorización legal o consentimiento del titular.

Por último, en el diseño de una ley de protección de datos cobra importancia la especificación de los ámbitos normados, ya sea comprendiendo únicamente a los registros automatizados o incluyendo a los convencionales; protegiendo o no a las personas jurídicas como titulares de datos personales; o abarcando únicamente al sector público, al privado o a ambos.

Estos pilares sobre los cuales se estructura una ley de protección de datos no siempre aparecen de un modo diáfano en la norma en estudio. En oportunidades se observa como la protección de la vida privada –que orientó desde sus orígenes la discusiones parlamentarias y a la que alude incluso la denominación de la Ley–, a veces en exceso, ante los derechos del responsable del registro, a causa de la insuficiencia de algunas garantías. También se aprecia cómo las disposiciones especiales para ciertos datos contenidos en fuentes accesibles al público quitan terreno a las normas generales de protección ordinaria.

También es necesario determinar si la Ley sigue el esquema de otros cuerpos normativos internacionales respecto al reconocimiento y tutela de determinadas facultades que se conceden al titular de los datos. En efecto, en las leyes de protección de datos el titular cuenta con un derecho para acceder a cierta información relevante que le concierne, piedra angular a partir de la cual es posible ejercitar otras facultades, como la rectificación, la cancelación o el bloqueo de los datos. Sin embargo, para hacer efectivo este derecho de acceso –y, consecuentemente, los otros–, se garantiza que el titular pueda saber quién está utilizando sus datos, para qué fines se están tratando, y si están siendo comunicados a terceros, gracias a que, previo al tratamiento, es necesario notificar este hecho a un órgano de control independiente, que mantiene un registro al efecto y cumple un rol fiscalizador y sancionador. Al respecto, estas leyes además contemplan un derecho al recurso –por vía administrativa, civil o, incluso, penal–, con sanciones y responsabilidades para quienes incumplan sus disposiciones.

Nos parece que el legislador sólo entendió una parte de este entramado, ya que se limitó a reconocer tales facultades, pero luego, las dejó carentes de eficacia práctica al no establecer la obligación de registro de los bancos de datos privados y al no crear un órgano especializado encargado de velar por el cumplimiento de la Ley.

Todo lo anterior, unido a otras omisiones graves, por ejemplo, en materia de seguridad, en la necesidad de consentimiento del titular para realizar las comunicaciones a terceros o en relación con la transferencia internacional de datos, lejos de tratarse de críticas meramente formales o de segundo orden, son errores esenciales del legislador que reafirman nuestra opinión sobre la Ley N° 19.628, y nos llevan a concluir que en Chile aún está pendiente el tema de la protección de datos personales.

## 5. Bibliografía

- Constitución Política del Estado de Chile
- Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado
- Ley N° 19.628, sobre Protección de la Vida Privada
- Diario de Sesiones del Senado, sesión 20ª ordinaria, de martes 5 de enero de 1993
- Herrera Bravo, Rodolfo y Núñez Romero, Alejandra. *Derecho Informático*. Editorial La Ley Ltda. Santiago, 1999.
- Suñé Llinás, Emilio. *Tratado de Derecho Informático*. Universidad Complutense. Volumen I. Madrid, 2000.
- Ull Pont, Eugenio. *Legislación Informática*. Universidad Nacional de Educación a Distancia. Segunda Edición. Madrid, 1999.

## 6. [Anexo 1](#): Ley N° 19.628

### LEY NUM. 19.628 SOBRE PROTECCION DE LA VIDA PRIVADA

Diario Oficial de 28/8/99

Ministerio Secretaría General de la Presidencia

PROTECCION DE DATOS DE CARACTER PERSONAL

## **Título Preliminar**

### **Disposiciones generales**

**Artículo 1º.-** El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

**Artículo 2º.-** Para los efectos de esta ley se entenderá por:

- a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.
- b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.
- c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.
- d) 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.
- e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
- f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
- h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
- i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.
- j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.
- k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.
- m) 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.
- n) Responsable del registro o banco de datos, 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.
- ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

o) 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.

**Artículo 3°.-** 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.

## **Título I**

### **De la utilización de datos personales**

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

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

La autorización debe constar por escrito.

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

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

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

**Artículo 5°.-** El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:

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

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

**Artículo 6°.-** Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

**Artículo 7°.-** Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

**Artículo 8°.-** En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales.

El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

**Artículo 9°.-** Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

**Artículo 10.-** No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

**Artículo 11.-** El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

## **Título II**

### **De los derechos de los titulares de datos**

**Artículo 12.-** 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.

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.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis

meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

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

**Artículo 13.-** El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

**Artículo 14.-** Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.

**Artículo 15.-** 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 del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.

Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva.

**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.

El procedimiento se sujetará a las reglas siguientes:

a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

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

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

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual

resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales.

La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decreta el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

### **Título III**

#### **De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial**

**Artículo 17.-** Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.

**Artículo 18.-** En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes.

**Artículo 19.-** El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente.

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

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

#### **Título IV**

##### **Del tratamiento de datos por los organismos públicos**

**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.

**Artículo 21.-** Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Exceptúase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7º, 11 y 18.

**Artículo 22.-** El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

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 que se produzca.

#### **Título V**

##### **De la responsabilidad por las infracciones a esta ley**

**Artículo 23.-** 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.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

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

#### **Título Final**

**Artículo 24.-** Agrégase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario:

"Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos."

#### **Disposiciones transitorias**

**Artículo 1º.-** Las disposiciones de esta ley, con excepción del artículo 22, entrarán en vigencia dentro del plazo de sesenta días, contados desde la fecha de su publicación en el Diario Oficial.

Los actuales registros o bancos de datos personales de organismos públicos se ajustarán a las disposiciones de este cuerpo legal, a contar de su entrada en vigencia.

Lo dispuesto en el artículo 22 comenzará a regir un año después de la publicación de esta ley. Sin perjuicio de lo anterior, los organismos públicos que tuvieren a su cargo bancos de datos personales deberán remitir los antecedentes a que se refiere dicho precepto con anterioridad, dentro del plazo que fije el reglamento.

**Artículo 2°.-** Los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la presente ley tendrán los derechos que ésta les confiere.

**Artículo 3°.-** Las normas que regulan el Boletín de Informaciones Comerciales creado por el decreto supremo de Hacienda N° 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley."

Habiéndose cumplido con lo establecido en el N° 1º del artículo 82 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévase a efecto como Ley de la República.

Santiago, 18 de agosto de 1999.- EDUARDO FREI RUIZ-TAGLE, Presidente de la República.- José Miguel Insulza Salinas, Ministro Secretario General de la Presidencia.- María Soledad Alvear Valenzuela, Ministra de Justicia.- Germán Quintana Peña, Ministro de Planificación y Cooperación.

Lo que transcribo a Ud., para su conocimiento.- Saluda Atte. a Ud., Carlos Carmona Santander, Subsecretario General de la Presidencia de la República.

### **Tribunal Constitucional**

#### **Proyecto de ley sobre protección de datos de carácter personal**

El Secretario del Tribunal Constitucional, quien suscribe, certifica que el Honorable Senado envió el proyecto de ley enunciado en el rubro, aprobado por el Congreso Nacional, a fin de que este Tribunal ejerciera el control de la constitucionalidad de su artículo 16; y que por sentencia de 4 de agosto de 1999, declaró:

1. Que los preceptos contenidos en el artículo 16, del proyecto sometido a control, son constitucionales en el entendido que deben interpretarse en conformidad con lo que se ha señalado en el considerando 7º de esta sentencia.
2. Que las disposiciones contempladas en el artículo 19 del proyecto sometido a control, son constitucionales.

Santiago, agosto 6 de 1999.- Rafael Larraín Cruz, Secretario.

### **7. Anexo 2: Decreto N° 779/2000, del Ministerio de Justicia**

#### **DECRETO N° 779/2000, del MINISTERIO DE JUSTICIA, SUBSECRETARIA DE JUSTICIA.**

Publicado en el Diario Oficial el 11 de noviembre de 2000

#### **APRUEBA REGLAMENTO DEL REGISTRO DE BANCOS DE DATOS PERSONALES A CARGO DE ORGANISMOS PUBLICOS**

Santiago, 24 de agosto de 2000.- Hoy se decretó lo que sigue:

Núm. 779.- Vistos: El artículo 32 N° 8 de la Constitución Política de la República y el artículo 22° de la ley N° 19.628, sobre Protección de la Vida Privada.

Decreto:

Apruébase el siguiente Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos.

**Artículo 1°.-** El Servicio de Registro Civil e Identificación llevará el Registro de los Bancos de Datos Personales a cargo de Organismos Públicos, en el cual se inscribirán todos los bancos de datos personales que de acuerdo con la ley respectiva lleven las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

### **TITULO I**

#### **De las Inscripciones en el Registro de Bancos de Datos Personales**

**Artículo 2°.-** Los organismos señalados en el artículo primero de este Reglamento deberán requerir su inscripción en el Registro de Bancos de Datos Personales ante las Oficinas del Servicio de Registro Civil e Identificación habilitadas para estos efectos o en el respectivo sitio en Internet del Servicio, o de cualquier otra forma que el Servicio determine.

Las inscripciones que sean requeridas a través del sitio en Internet del Servicio, estarán sujetas a las confirmaciones y medidas de seguridad que la institución determine conforme a las normas legales pertinentes.

**Artículo 3°.-** La inscripción en el Registro de Bancos de Datos Personales deberá contener, a lo menos, las siguientes menciones:

- 1.-El nombre del banco de datos personales;
- 2.-El organismo público responsable del banco de datos personales respectivo;
- 3.-El RUT correspondiente al organismo público;
- 4.-El fundamento jurídico de la existencia del banco de datos personales;
- 5.-La finalidad del banco de datos;
- 6.-El o los tipos de datos almacenados en dicho banco, y
- 7.-Una descripción del universo de personas que comprende.

**Artículo 4°.-** El Servicio de Registro Civil e Identificación otorgará al organismo público responsable de bancos de datos personales una certificación que indique a lo menos, el nombre y el RUT de dicho organismo, la individualización de cada uno de los bancos que se encuentren inscritos bajo su nombre en el respectivo Registro a la fecha de emisión del certificado y la fecha en que fueron registrados.

**Artículo 5°.-** Mediante resolución del Director Nacional se fijará el procedimiento de inscripción de los bancos de datos personales a cargo de los organismos citados en el artículo primero del presente reglamento.

## **TITULO II**

### **De las Obligaciones de los Organismos Públicos Responsables de Bancos de Datos Personales**

**Artículo 6°.-** Los organismos públicos que a la fecha de entrada en vigencia del presente Reglamento mantengan bancos de datos personales, deberán proceder a su inscripción en el Registro de que trata este reglamento, dentro del plazo de tres meses, contados desde igual fecha.

Los organismos públicos que se hagan responsables de nuevos bancos de datos personales, deberán proceder a su inscripción, dentro del plazo de 15 días contados desde que se inicien las actividades del respectivo banco de datos.

Toda modificación que se refiera a los bancos de datos personales ya registrados, deberá sujetarse a lo establecido en el artículo 9° del presente reglamento.

## **TITULO III**

### **De los Informes**

**Artículo 7°.-** El Servicio de Registro Civil e Identificación otorgará, por medios electrónicos, a todo el que lo solicite, un informe en el cual conste el nombre de un determinado banco de datos personales, las menciones acerca de la información que contiene y el nombre del organismo público responsable de su registro.

## **TITULO IV**

### **De las Correcciones y las Modificaciones**

**Artículo 8°.-** Cualquier corrección relativa a errores u omisiones de una inscripción, será requerida por el propio organismo responsable de dicha inscripción en el Registro de Bancos de Datos Personales, debiendo efectuarse de las formas establecidas en el artículo 2° del presente reglamento.

**Artículo 9°.-** Cualquier modificación de una inscripción, será requerida por el propio organismo responsable de dicha inscripción en el Registro de Bancos de Datos Personales, en el plazo de quince días contados desde que se produzca, debiendo efectuarse en alguna de las formas establecidas en el artículo 2° del presente reglamento.

Tómese razón, comuníquese y publíquese.- RICARDO LAGOS ESCOBAR,  
Presidente de la República.- José Antonio Gómez Urrutia, Ministro de Justicia

---

**CITAS BIBLIOGRAFICAS.**

(1) El Constituyente ha entendido en este precepto que el concepto "vida privada" está directamente vinculado a la intimidad, ya que en la sesión 129 de la Comisión de Estudios para la Nueva Constitución, Silva Bascuñan, al trabajar sobre esta garantía señaló: *Para completar la explicación de la sustancia de este precepto, deseo poner de relieve su trascendencia en este momento que vive el mundo. Por un lado, el proceso de socialización ha producido una interpenetración enorme entre la persona y la sociedad, y ya no puede concebirse el desarrollo de la persona humana en forma aislada o individual. Por otra parte, la sociedad influye enormemente y determina en muchos aspectos al individuo [... Así.] frente a una sociedad que [...] abruma al hombre dentro de la riqueza de los medios que tiene para influir sobre él, es terriblemente dañino que la sociedad se masifique totalmente en un proceso en el cual los valores superiores no sean puestos de relieve. ¿Y de dónde va a surgir la posibilidad de que se coloquen en términos verdaderamente de influencia los valores superiores del individuo? En la misma proporción en que se le reserve al hombre un santuario de intimidad en el cual pueda formar, producir, consolidar y desarrollar esos valores que después va a expresar en la sociedad. Si no se le deja al individuo ninguna intimidad, entonces la sociedad se va a masificar en una serie de individuos sin ninguna posibilidad de aportar algo de progreso, algo de perfeccionamiento a la sociedad entera.*

Ahora bien, sobre el respeto a la "vida pública" que reconoce la Constitución, la idea es cautelar las actuaciones de las personas que, por su naturaleza, deban o puedan ser conocidas por la sociedad, para evitar la imputación de hechos falsos que injustificadamente causen daño o descrédito a una persona o a su familia.

(2) El anglicismo "privacidad" es un concepto desafortunado que no se justifica al existir las expresiones "intimidad" o "vida privada", por lo cual su utilización no es correcta.

(3) Diario de Sesiones del Senado, sesión 20ª ordinaria, de martes 5 de enero de 1993. Pág. 3.082.

(4) El artículo 8, inciso 2, del Proyecto de Ley del Senado entendía por informática a *"las operaciones realizadas por medios automáticos, relativos a la recogida, registro, elaboración, modificación, conservación y destrucción de informaciones, así como las operaciones de la misma naturaleza referentes a la explotación de ficheros o bases de datos y a las interconexiones o cotejos, consultas o comunicaciones de informaciones"*.

(5) Artículo 2 letra ñ, de la Ley.

(6) Artículo 2 letra n, de la Ley.

(7) Artículo 2 letra k, de la Ley.

(8) El inciso segundo del artículo 1 de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado dispone: *"La Administración del Estado estará constituida por los Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por Ley"*.

(9) Figura contemplada en 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.

(10) Artículo 2 letra o, de la Ley.

(11) Artículo 2 letra m, de la Ley.

(12) Artículo 2 letra a, de la Ley.

(13) Artículo 2 letra j, de la Ley.

(14) Artículo 2 letra c, de la Ley.

(15) Artículo 2 letra l, de la Ley.

(16) Artículo 2 letra e, de la Ley.

(17) Artículo 2 letra b, de la Ley.

(18) Artículo 2 letra h, de la Ley.

(19) Artículo 2 letra f, de la Ley.

(20) Artículo 2 letra g, de la Ley.

(21) Artículo 6, Convenio 108 del Consejo de Europa, en Estrasburgo, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

(22) Artículo 8, 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.

(23) En otras Leyes se trata el tema de manera similar. La Ley Federal de Austria, sobre Protección de Datos de carácter personal, define en el artículo 2 a los "Datos sensibles o Datos especialmente dignos de protección, como *"Datos de las personas físicas, relativos a su origen racial y étnico, opinión política, afiliación sindical, convicción religiosa o filosófica, salud o vida sexual"*; la parte preliminar de la Ley Británica sobre protección de datos se entiende por datos personales sensibles a *"los que contuvieren información referente a: el origen racial o étnico del interesado; sus opiniones políticas; sus creencias*

*religiosas u otras creencias de naturaleza similar; su pertenencia a un sindicato (según lo definido en la Ley (Refundida) de Sindicatos y Relaciones Laborales de 1992); su salud o condición física o mental; su vida sexual; la comisión o la supuesta comisión de una infracción por su parte; o cualquier procedimiento por cualquier infracción cometida, o supuestamente cometida, por él; la resolución de dicho procedimiento o la sentencia de cualquier tribunal en dicho procedimiento"*; el texto consolidado de la Ley 675/1996, de Italia, sobre Protección de las personas y otros sujetos por lo que atañe al tratamiento de datos personales, establece en el artículo 22 que *"los datos personales que fueren idóneos para revelar el origen racial y étnico, las convicciones religiosas, filosóficas o de otra índole, las opiniones políticas, la adhesión a partidos, sindicatos, asociaciones u organizaciones con carácter religioso, filosófico, político o sindical, así como los datos idóneos para revelar el estado de salud o la vida sexual, podrán ser objeto de tratamiento sólo mediante el consentimiento previo, dado por escrito del interesado, y previa autorización de la Autoridad de control"*; y la Ley Sueca 204, de 1998, sobre protección de datos de carácter personal señala en el artículo 13, que *"Queda prohibido el tratamiento de datos que revele: Raza u origen*

racial; Ideología/opiniones políticas; Creencias religiosas o filosóficas; Afiliación sindical. Queda también prohibido el tratamiento de datos relativos a la salud o a la vida sexual”.

(24) Véase el artículo 10 de la Ley N° 19.628.

(25) Al mencionar los hábitos personales se abre un abanico de posibilidades enormemente amplio, por lo que es necesario limitarlos únicamente a los que integran la esfera íntima del individuo.

(26) Artículo 2 letra d, de la Ley.

(27) Artículo 2 letra i, de la Ley.

(28) Véase el artículo 24 de la Ley N° 19.628.

(29) El artículo 19 N° 12 de la Constitución Política establece: “La Constitución asegura 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”.

(30) Véase el artículo 1 de la Ley N° 19.628.

(31) Lo correcto es ejercitar este derecho frente al responsable del registro, sin embargo, la Ley dispone en el artículo 14: “Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos”.

(32) Véase el artículo 12, inciso 1, de la Ley N° 19.628.

(33) La Ley utiliza las expresiones “modificación” y “eliminación”, en vez de “rectificación” y “cancelación”, pero nosotros emplearemos preferentemente estas últimas, por ser más habituales en la doctrina y el derecho extranjero.

(34) Véase el artículo 12, incisos 2 y 3, de la Ley N° 19.628.

(35) Véase el artículo 4, inciso 4, de la Ley N° 19.628.

(36) Véase el artículo 12, inciso 4, de la Ley N° 19.628.

(37) Véase el artículo 3 de la Ley N° 19.628.

(38) Véase el artículo 12, inciso 5, de la Ley N° 19.628.

(39) El artículo 16 de la Ley señala reglas a las que se sujetará el procedimiento para solicitar amparo de estos derechos ante los tribunales, sin embargo, no las analizaremos en este trabajo.

(40) Véase el artículo 6 de la Ley N° 19.628.

(41) Véase el artículo 12, inciso 6, de la Ley N° 19.628.

(42) Véase el artículo 15 de la Ley N° 19.628.

(43) Véase el artículo 23 de la Ley N° 19.628.

(44) Véanse los artículos 4 y 20 de la Ley N° 19.628.

(45) Véanse los artículos 18 y 19, inciso 1, de la Ley N° 19.628.

(46) Véase el artículo 19 de la Ley N° 19.628.

(47) Véase el artículo 9 de la Ley N° 19.628.

(48) Véanse los artículos 7 y 11 de la Ley N° 19.628.

(49) Para definir estos aspectos y cumplir el mandato legal que existía en tal sentido, se dictó el decreto N° 779/2000, del Ministerio de Justicia, publicado en el Diario Oficial el 11 de noviembre de 2000, que aprueba el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos. Su texto se transcribe en el anexo 2 de este trabajo.