



Comentarios al articulado del Proyecto de Ley que modifica la Ley N° 19.628, sobre protección a la vida privada¹

Artículo 1° Objeto:

- El proyecto señala que la ley tiene por objeto la protección de los datos personales, a fin de asegurar a las personas el legítimo ejercicio del derecho de protección a la vida privada garantizado en el número 4° del Art. 19 de la Constitución. Al respecto, hoy en día se reconoce la protección de datos como un derecho humano independiente y autónomo de la privacidad o intimidad, una garantía de protección y control de los datos personales que nos conciernen frente a su tratamiento automatizado, el que realizado de manera indiscriminada e ilegítima puede afectar no sólo a la intimidad, sino una serie de derechos fundamentales. Debe entenderse que los datos personales no son aislados de la persona de su titular sino componentes e integrantes de ésta, constituyendo su individualidad y personalidad. Cada vez que se procesan datos personales, procesamos a la persona misma y a sus derechos fundamentales.
- En sintonía a lo expresado, no compartimos la idea de extender la protección a las personas jurídicas, puesto que la protección de datos, es un derecho humano, consagrado incluso constitucionalmente en otras legislaciones.
- Por otra parte, pareciera ser privilegiada la protección otorgada en la norma a las personas jurídicas al hablar de *“derechos acorde a su naturaleza le resulten aplicables* y no restringirlo a un derecho concreto, como el de la intimidad en el caso de las personas físicas.
- Estimamos la inconveniencia de eliminar parte del actual inciso primero referido al ejercicio de las libertades de emitir opinión y de informar, puesto que una de las excepciones al tratamiento de datos debe ser la libertad de expresión, sólo en la

¹ Elaborado por **Romina Garrido Iglesias**. Abogada Universidad de Valparaíso. Diplomada en Derecho Informático en la Facultad de Derecho de la U. de Chile. Magíster © en Derecho Informático y Telecomunicaciones en la misma Universidad; y **Jessica Matus Arenas**. Abogada Universidad de Chile. Diplomada en Derecho Informático en la Facultad de Derecho de la U. de Chile. Magíster © en Derecho Informático y Telecomunicaciones en la misma Universidad. Coautora del libro “La cesión de datos personales”, Editorial Lexis Nexis, 2006. Ambas creadoras del sitio www.protecciondedatospersonales.cl y miembros de la Red Iberoamericana de Protección de Datos.



medida que resulte necesario para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión².

Artículo 2° Definiciones:

- Falta incorporar las definiciones del derecho de oposición y de rectificación
- No hay mejora a los conceptos de datos personales ni de datos sensibles, se limita a reemplazar el vocablo “información” por “dato”. Se podría aprovechar esta instancia para incorporar expresamente como dato sensible los datos de menores de edad. Por otro lado, estimamos correcto no limitar los casos para calificar una determinada situación como datos sensible.
- La ley restringe su ámbito de aplicación de acuerdo a los órganos que podrán conocer las sanciones, se excluye a órganos anteriormente incluidos (ley actual habla hoy de organismos públicos en general)
- Es necesario y relevante mejorar la definición de “fuente de acceso público”, que es confusa en la ley actual. Pareciera indicar que la determinación del acceso público se entrega al responsable de la base de datos, no determinándose de acuerdo a la fuente o naturaleza del dato esencialmente público.
- Se señala que se incorpora una letra r) nueva sin contenido.

Artículo 3° Principios:

- Los principios generales definen pautas a las que debe atenerse en la recolección, tratamiento y uso de los datos, encaminadas a garantizar tanto la veracidad de la información registrada como la congruencia y racionalidad de la utilización de los datos. La calidad del dato es fundamental como principio.
- No se incorpora el Principio de Control en las definiciones.
- En la definición de calidad, falta incorporar los atributos de “real y veraces” en el sentido de responder a la realidad actual de su titular.

² En España por ejemplo, el uso de datos personales en las noticias publicadas debe cumplir tres requisitos: ser un “hecho noticioso”, ser veraz y ser necesaria la publicación de los datos. Este último requisito es el que ha dado lugar a varias resoluciones sancionadoras ratificadas por los tribunales españoles.

Protección de Datos Personales

<http://protecciondedatospersonales.cl>

<http://twitter.com/datospersonales>



- Los principios de especificación y limitación de uso, deberían apuntar a un solo concepto, esto es, al principio de finalidad, en el sentido que ambos son integrantes de éste.
- El artículo confunde principios y derechos, señalando como principios el de acceso y oposición, el de transparencia, y el de información, en circunstancias que éstos son todos derechos del titular de los datos.
- Deben incorporarse los principios de temporalidad, confidencialidad, ubicuidad y debida diligencia y sus definiciones.
- En la información como derecho (letra h), es fundamental informar sobre la finalidad en el tratamiento.

Artículo 4° Consentimiento:

- La licitud se basa en la información, no basta que sólo conste el consentimiento, el consentimiento debe ser “informado”.
- No incorpora los atributos de tiempo y espacio: duración del tratamiento y obligatoriedad en el territorio.
- La incorporación de consentimientos generales y otros de carácter específicos se traducen en contratos de adhesión con consentimientos generales que autorizarán cesiones indiscriminadas de datos personales.
- Respecto a que la revocación del consentimiento conste por algún medio no debiera limitarse a un medio físico o tecnológico, si no a cualquier medio en general.

Artículo 4° A) Excepciones al consentimiento:

- Letra a); hace referencia a la fuente accesible a público, concepto que debe mejorarse.
- Letra d); es indispensable incluir la pertinencia del dato. Pensemos que en general nos enfrentamos a contratos de adhesión en estos casos.



- Letra f); la urgencia médica dará pie para legalizar que las clínicas pidan el DICOM para hospitalizar, puesto que en los términos en que está redactada la norma se señala que el tratamiento de datos (en general) debe resultar necesario en caso de urgencia médica.
- Letra g); postulamos su eliminación pues corresponde a una materia tratada en otro proyecto de ley, relativo a obligaciones financieras y comerciales
- La parte final debe incluir no sólo al destinatario sino a todos los cesionarios.

Artículo 4° B) Deber de información y sus contenidos:

- Sugerimos eliminar la referencia a los formatos en que puede constar la información al momento de la recolección, dejando la norma lo más neutra posible.
- Se sugiere reemplazar la frase “al momento de la recolección” por la siguiente “en toda solicitud de datos”.
- En la letra c) se deben consagrar todos los derechos que le asisten al titular, faltando cancelación, bloqueo y rectificación. El derecho de oposición establecido en el literal no es definido en el art. 2° de la ley.

Artículo 5° A) Norma general para la transferencia internacional de datos.

Esta disposición no soluciona la condición de nuestro país como no adecuado en materia de protección de datos. La norma en el proyecto establecida no permitiría a Chile ser declarado país con un nivel adecuado de protección por parte de la Unión Europea. Si bien la Directiva Europea se encuentra en actual revisión en cuanto al procedimiento de adecuación, creemos que dicho estudio no reducirá el estándar de derechos que las legislaciones deben consagrar. El sistema propuesto es un modelo equivalente y contractual, finalmente de autorregulación. Se entrega a las entidades el cumplimiento de un determinado nivel de protección, no la normativa de los países importadores del dato.

Artículo 6° Eliminación, modificación y bloqueo de datos.

El artículo no da parámetros para la temporalidad del dato.



Artículo 7° Deber de secreto:

Se propone excluir la excepción de fuente accesible al público en el deber de confidencialidad.

Artículo 9° Deber de informar registros y bancos de datos:

- Llama la atención que una norma de protección de datos disponga de la publicidad de registros de proveedores, clientes y personal que labora (desprotegiendo sus datos o valorándolos menos) y, más aún, de un motor de búsqueda que permita indexar datos personales para ser consultados por sus titulares, cosa sobre la cual no se tiene control preciso y exclusivo que serán sólo consultados por éstos. No hay claridad en la excepción establecida en el inciso cuarto.
- Un Registro de Bases de Datos por parte de particulares debiera ser una de las obligaciones del órgano de control, el que no es creado por el proyecto.

Artículo 10 Deber de información

- El inciso segundo debiera hacer obligatorio un control de acceso exclusivo para cada titular del dato.

Artículo 11 Tratamiento de datos sensibles:

- El inciso tercero es muy amplio, debiese remitirse sólo a aquellos casos en que una ley autorice el tratamiento de datos sensibles.

Artículo 11 A) Medidas de seguridad:

- ¿Debemos entender que en el caso de órganos públicos se refiere al DTO 83/2004?, norma que por cierto debe actualizarse.
- Respecto a los privados ¿qué normativa se aplica? ¿Cuál es el estándar? ¿De qué manera se uniforman criterios?

Protección de Datos Personales

<http://protecciondedatospersonales.cl>

<http://twitter.com/datospersonales>



Artículo 2 Derecho de acceso:

- Se amplía el plazo de 2a 5 días hábiles contemplado en la ley actual para responder a una solicitud de acceso al dato.

Artículo 13: Derecho de oposición.

- Falta definir este derecho en el artículo 2° de la ley.
- Falta consagrar la ubicuidad
- La norma no aclara si la oposición debe hacerse por escrito o por otro medio que el responsable disponga.
- El plazo de 15 días hábiles es excesivo, en la medida que no se establezca por ley el bloqueo del dato (no cesión a terceros) que está siendo controvertido mientras dura el procedimiento de oposición.

Artículo 16 A) Procedimiento de reclamo contra un organismo público y 16 B) entidades privadas:

- No compartimos la visión que sea el organismo encargado de velar por el acceso a la información pública, el encargado de velar por la protección de los datos personales, puesto que se trata de dos derechos diversos.
- Tampoco compartimos que los privados deban dirigirse a un órgano distinto, como el SERNAC, en el conocimiento de los reclamos. Se requiere una institucionalidad en materia de protección de datos aplicable tanto a públicos como privados. Dos organismos cuya naturaleza es diferente torna difícil la unificación de criterios.
- Los datos personales como lo mencionamos al inicio personales no son aislados de la persona de su titular sino componentes e integrantes de éste, constituyendo su individualidad y personalidad. Cada vez que se procesan datos personales, procesamos a la persona misma y a sus derechos fundamentales, debiendo consagrarse sanciones igualitarias en el caso de públicos y privados.



- El procedimiento civil contemplado no se condice con la realidad actual de los juzgados civiles, puesto que éstos no realizan notificaciones electrónicas.
- Por otra parte, se mantiene el peso de la prueba en el titular del dato, quien en la mayoría de los casos no contará con los medios de prueba suficientes. La regla es a la inversa, quien realiza tratamiento de datos es el que debe probar que lo hizo con la debida diligencia.
- La consagración práctica y efectiva del principio de control en la protección de datos, supone la existencia de una autoridad independiente u órgano de control. Así se observa y lo disponen el Tratado de la Unión Europea, Tratado Constitutivo de la Unión y la Carta de los Derechos Fundamentales de la UE. La independencia de esta autoridad se traduce en una independencia de nombramiento y presupuestaria, con funciones normativas, de intervención y de investigación concretas (tanto preventivas como sancionatorias a posteriori) y consagradas en la ley que la regula, que en el caso chileno no ocurre. También es necesario que la autoridad posea facultades de supervisión sobre la actividad de tratamiento, no siendo suficiente la expresión “velar por” que hoy está contenido en la letra m) del artículo 33 de la ley de Transparencia y que se pretende incorporar al Art. 58 de la ley del consumidor. Esta frase conduce y ha conducido en el caso del Consejo para Transparencia a ambigüedades sobre las verdaderas potestades del órgano en la materia y hasta dónde puede llegar en el conocimiento y en la regulación del tema para el sector público o el privado. Finalmente, la autoridad es el reconocimiento del derecho a la protección de datos como derecho autónomo, y delegar o traspasar las competencias en organismos que han sido creados con otras competencias, con funciones distintas, con finalidades diferentes, apunta en una dirección que desconoce el derecho en su esencia,

Advertimos que las nuevas legislaciones de países del entorno han creado instituciones que velan por la protección de datos, así por ejemplo, la Dirección nacional de Protección de Datos Personales (Argentina), la Unidad Reguladora y de Control de Datos Personales (Uruguay), una Agencia de Protección de Datos (Perú), próxima a constituirse, y otra en Costa Rica, también por implementarse (su ley se publicó en septiembre de 2011). En general, estas instituciones dependen del Ministerio de Justicia.



Artículo 20 Tratamiento de datos órganos públicos:

- El proyecto no indica cuál es el plazo para que los órganos públicos adecuen su ley orgánica a la presente normativa.
- El inciso 1° señala que el tratamiento de datos deberá efectuarse “con sujeción a las reglas dispuestas en su propia ley orgánica, en caso que las tuviera, o en su defecto a las normas especiales que establece esta ley”, en circunstancias que debiese mantenerse la redacción actual “con sujeción a las reglas precedentes”. Lo anterior, por cuanto la ley de protección de datos establece los principios básicos que deben observarse en cualquier tratamiento, ya sea por un público o un privado; otorga derechos a los titulares e impone obligaciones a los responsables de bases de datos. Si se quiere determinar con mayor precisión cuándo un órgano público puede tratar datos, debiese complementarse el concepto de “competencia” del órgano, puesto que la competencia está dada por su respectiva ley orgánica, siendo la Ley 19.628 el paraguas legal para el tratamiento de datos de cualquier organismo, a falta de ley especial. El inciso 3° de dicho artículo debe indicar expresamente también que los titulares de los datos pueden ejercer, frente a los órganos públicos, su derecho de rectificación, bloqueo o cancelación cuando corresponda.

Artículo 24 Sanciones:

- El modelo sancionatorio debe contemplar sanciones más severas, de manera que sean persuasivas. En este sentido, establecer las sanciones leves en rango de 1 a 20 UTM, por ejemplo, no permite desincentivar que las empresas asuman los costos de multas como costos internos. Por otra parte, debe considerarse que se trata del principal activo de las empresas y del Estado: datos personales.
- ¿Cómo las personas van a probar que se incumplió la protección si en ellas recae el peso de la prueba?

Artículo 27 Modelo de prevención:

- No queda claro quién lo supervisa y si la norma aplica a públicos y a privados.

Protección de Datos Personales

<http://protecciondedatospersonales.cl>

<http://twitter.com/datospersonales>



- Surge la pregunta acerca de cómo se compatibiliza este modelo con el encargado de seguridad del DTO 83/2004 en el caso de los órganos públicos.
- El arbitraje ¿se aplica para los públicos y privados por igual? ¿Qué institución regulará lo anterior?
- Se vislumbra que los contratos de adhesión traigan incorporadas cláusulas de arbitraje “voluntario” que se transformará en obligatorio al aceptar las condiciones.

Artículo 29 Contrato de Certificación de Modelo de Prevención:

- El inciso 1° sólo señala al “responsable del tratamiento de datos”, debe tratarse de un error puesto que los sujetos son “responsable de la base de datos” y “encargado del tratamiento”.

Artículo 30 Sanciones accesorias:

- Cuando la norma señala que puede disponerse además la suspensión de las operaciones del registro hasta por un término de seis meses, debiera indicar además que frente a esta suspensión se produce el bloqueo de los datos.

Art. 32 Derecho a indemnización:

- En el inciso primero se deja fuera al encargado del tratamiento, que como bien se señala en el inciso 3° del mismo artículo, responde solidariamente.

Art. 33 Propuestas de acuerdos reparatorios:

- La norma hace referencia a “todos los titulares afectados por la misma situación”, entendiéndose por tanto que debe tratarse de acuerdos colectivos. Esta modalidad de solución de conflicto debiera también establecerse de manera expresa para aquel titular individualmente considerado.

Consideraciones generales del proyecto:

Indudable resulta concluir que nuestro país requiere una reforma urgente a su normativa de protección de datos personales, con el objeto de no sólo dar cumplimiento a los

Protección de Datos Personales

<http://protecciondedatospersonales.cl>

<http://twitter.com/datospersonales>



estándares internacionales europeos en la materia, sino que también convertirse, conforme a lo anterior, en un país atractivo para invertir en él.

Esta fue sido la preocupación de las autoridades nacionales que presentaron el proyecto de ley que modificaba la Ley 19.628 (Boletín 6120), al verse envueltos en un escenario que no permitiría la atracción de inversiones extranjeras, en lo que el Consejo Nacional de Innovación ha denominado Cluster de Offshoring, esto es, concretar en Chile una plataforma de servicios a distancia, identificada como una de las de mayor potencial de crecimiento durante la próxima década.

Mientras Chile no sea declarado país con protección adecuada por la Unión Europea, deberá intentar que los contratos que se suscriban en lo sucesivo logren las respectivas autorizaciones con rapidez para no quedar desfasados en el comercio internacional respecto del rubro de las Tecnologías de la Información.

Respecto de las autorizaciones se debe dimensionar la importancia que éstas tienen para la economía de nuestro país, puesto que muchas veces las empresas europeas optan por contratar, en Latinoamérica, con compañías argentinas. Atendido el hecho de ser un país adecuado conforme a la Comisión Europea, las transferencias internacionales de datos personales no requieren de dicha autorización –cuya tramitación no es menor–, sino simplemente de la notificación de la transferencia a fin de proceder a su inscripción en el Registro General de Protección de Datos. Algunas estadísticas³ permitirán, en definitiva, observar el panorama general al 31 de marzo de 2011:

³ RUBÍ NAVARRETE, Jesús (Adjunto al Director de la Agencia Española de Protección de Datos). “El impacto de las transferencias internacionales de datos en américa latina. las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos”. Ponencia en Seminario del mismo nombre, Colombia, 14 al 16 de junio de 2011 [en línea] Fuente: <http://www.redipd.org/reuniones/seminario_2011_Cartagena/common/Ponencias/JesusRubi_1_Transferencia_internacional.pdf> [consulta 20 de septiembre de 2011].

Protección de Datos Personales

<http://protecciondedatospersonales.cl>

<http://twitter.com/datospersonales>



- Paso 2: Iniciativa del país. El país interesado debe enviar una solicitud oficial a la Comisión Europea, mediante una carta del embajador del país aspirante al Comisario y el Director General de la Dirección General Justicia, Libertad, Seguridad. Conjuntamente, debe enviarse la ley nacional de protección de datos traducida a distintos idiomas, siendo conveniente, además, enviar las aclaraciones de los documentos cuando se trate de palabras o término que no signifiquen o representen necesariamente lo mismo en los diversos países de habla hispana, en nuestro caso.
- Paso 3: Análisis de la Comisión Europea. Existe en primer lugar un diálogo con el país interesado respecto de sus textos normativos. Luego, se realizan Estudios –que se encomiendan a Universidades– que describen al país y su sistema de protección de datos. Posteriormente, se informa al Grupo de Trabajo del artículo 29
- Paso 4: Grupo de trabajo artículo 29. Este órgano emite un Dictamen sobre el nivel de adecuación del peticionario, como los ya mencionados en este estudio, que debe enviarse a la Comisión Europea.
- Paso 5: Preparación de un borrador de la decisión de adecuación por parte de la Comisión. La elaboración de este borrador implica su traducción en los 23 idiomas oficiales de la Unión Europea.
- Paso 6: Comité de representantes de los gobiernos de los Estados miembros. Este Comité mediante un Dictamen aprueba el texto preliminar de la Decisión de la Comisión Europea.
- Paso 7: Parlamento Europeo. El Parlamento cuenta con 30 días para reflexionar sobre el borrador y emitir, si lo considera, un Dictamen.
- Paso 8: Supervisor Europeo de Protección de Datos. También tiene la posibilidad de ofrecer un dictamen.
- Paso 9: Decisión de la Comisión Europea. Se trata de adopción formal de la Decisión de adecuación, que se transmite a los Estados miembros, y tiene efecto jurídico inmediato, publicándose en el Diario Oficial de la Unión Europea.

Actualmente, son válidas las transferencias internacionales de datos efectuadas a los Estados miembros de la Unión Europea, a los Estados miembros del Espacio Económico Europeo y a los Estados cuya adecuación haya sido declarada por la Comisión Europea: Estados Unidos (2000), Suiza (2000), Canadá (2001), Guernsey (2003), Isla de Man (2004), Argentina (2003), Jersey (2008) y Andorra (2010). Uruguay se encuentra en proceso de adecuación.