Principales cambios sufridos en el Proyecto de Ley
durante la tramitación en la Comisión de Constitución del Senado.

Boletín 11.092 y 11.144 Refundidos.

I. Ámbito de aplicación.

- El Proyecto de Ley evoluciona desde un modelo donde la Ley 19.628 era supletoria de las regulaciones sectoriales, a un sistema en que todo tratamiento de datos que realicen personas naturales y jurídicas, incluidos los órganos públicos, quedan regidos por la Ley 19.628.

II. Definiciones.

Se perfeccionan la redacción de la definición de:

a. Comunicación o transmisión de datos personales. Se eliminan elementos que no eran propios de una definición, como lo son las características de veracidad, exactitud, completitud y veracidad, que son requisitos que deben cumplir los datos personales tratados en cualquier operación de tratamiento.
b. Dato personal. Se precisa que la identificación de la persona puede realizarse a través de uno o más identificadores. Anteriormente se señalaba que sólo podía ser un identificador.
c. Fuentes de acceso público. Se listan ejemplos de esta clase de fuentes (listas de colegios profesionales, diario oficial, medios de comunicación o los registros públicos que disponga la ley). Lo relevante de esto es que se asigna a la autoridad de protección de datos el deber de listar las fuentes de acceso público, lo que impacta en la posibilidad de recurrir a esta clase de fuentes para tratar datos sin el consentimiento del titular.
d. Derecho de rectificación. Se precisa que el derecho también aplica cuando los datos se encuentran desactualizados.
e. Registro Nacional de Cumplimiento y Sanciones: Se precisa que sólo se registran los modelos que estén certificados y se agrega que se registrarán a los responsables que hayan adoptado los modelos y también aquellos a los que se les ha revocado la certificación.

Se incorpora la definición de:

a. Anonimización o disociación. Se indica que se trata de una técnica a través de la cual se destruye o eliminado el nexo de la información que vincula, asocia o identifica con una persona determinada. Un dato anonimizado deja de ser un dato personal.
b. Seudonimización. Se indica que es el tratamiento de datos que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.

c. Cesión de datos personales. Se señala que es la transferencia de los datos a otro responsable.
d. Elaboración de perfiles. Se dispone que es toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural. Esta definición sólo se utiliza con ocasión del derecho de oposición a valoraciones personales automatizadas.
e. Tercero mandatario o encargado. Se dispone que es la persona que trata datos personales, por cuenta del responsable de datos.

III. Derechos de los titulares.

- Se precisa, en el artículo 4 inciso 4º, que los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.
- Se precisa, en el artículo 11 inciso 7º que la rectificación, cancelación u oposición al tratamiento de los datos se aplicará sólo respecto de los responsables a quienes se les haya formulado la solicitud. Con todo, cuando el responsable haya comunicado dichos datos a otras personas, deberá comunicar a éstas los cambios realizados en virtud de la rectificación.
- Se precisa que una vez rectificados los datos no podrá volver a tratar los datos sin rectificar.
- En el derecho de oposición para marketing se precisa que la oposición tiene como límite que el titular haya dado el consentimiento en un contrato para que especialmente le envíen comunicaciones de esta clase.
- Se elimina el derecho de oposición efectuada por los herederos.
- En el derecho de oposición a valoraciones personales automatizadas se elimina el requisito de que para oponerse las valoraciones debían afectar significativamente en forma negativa o producir efectos jurídicos adversos. Ahora el derecho es absoluto.
- El derecho a la portabilidad se simplifican los requisitos para su ejercicio, estableciendo que este derecho aplica solo respecto a los datos que hubiera aportado el titular y el tratamiento se realice en forma automatizada y basado en el consentimiento del titular. Así, se elimina que se trate de un volumen relevante de datos. Asimismo, se elimina el deber del responsable de utilizar los medios más expeditos, menos onerosos y sin poner trabas u obstáculos para el ejercicio de este derecho y que debe comunicar al titular de manera clara y precisa las medidas necesarias para recuperar sus datos personales y especificar las características técnicas para llevar a cabo estas operaciones.
- Se permite que el responsable pueda exigir el pago de los costos directos en que incurra, cuando el titular ejerza su derecho de acceso más de una vez en el trimestre o cuando ejerza el derecho a la portabilidad. Sin embargo, se precisa que los parámetros

y mecanismos para determinar los costos derivados del ejercicio de los derechos serán determinados por la autoridad de protección de datos, a través de una instrucción general que considerará, entre otros antecedentes, el volumen de los datos a ser entregados, la naturaleza jurídica y el tamaño de la entidad o empresa que tenga la calidad de responsable.

IV. Principios del tratamiento.

Licitud.

- Respecto del tratamiento de datos que se realiza sin consentimiento del titular a partir de datos recolectados de fuentes de acceso público se elimina el deber de que el tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos. Sin embargo, se debe tener presente que el Proyecto migró hacia un modelo en que es la autoridad de protección de datos la que deberá listar cuales son las fuentes de acceso público.

Finalidad.

- Inicialmente el tratamiento de datos se podía hacer para fines diferentes a los informados al momento de la recolección cuando existiera una relación contractual o precontractual entre el titular y el responsable que justificara el tratamiento con una finalidad diferente. Con el texto aprobado en la Comisión se restringe la hipótesis señalada ya que la finalidad diferente debe enmarcarse en los fines del contrato o, ser coherente con las tratativas o negociaciones previas a la celebración de este.

Principio de seguridad.

- Se agrega que los estándares de seguridad deben proteger los datos contra tratamientos ilícitos.
- Junto a ello se precisa que las medidas deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.
- Adicionalmente, se agrega que las medidas deben adoptarse considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos. Asimismo, deberán evitar la alteración, destrucción, pérdida, tratamiento o acceso no autorizado.
- Se precisa que si las bases de datos que opera el responsable tienen distintos niveles de riesgo, deberá adoptar las medidas de seguridad que correspondan al nivel más alto.
- Se mantiene alterada la carga de la prueba en caso que ocurrencia de un incidente de seguridad, ya que es el responsable quien deberá acreditar la existencia y el

funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgo y a la tecnología disponible.
- Se establece que un Reglamento deberá establecer los estándares de cumplimiento y medidas mínimas, comunes para todos los responsables.

Principio de confidencialidad.
- Se elimina la obligación de confidencialidad del responsable respecto de los datos que trata cuando provienen de fuentes de acceso público.

V. Responsable no domiciliado en Chile.
- Se establece la obligación para el responsable no domiciliado en Chile que trata datos de residentes de Chile de señalar y mantener actualizado y operativo, un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y de la Agencia de Protección de Datos Personales.

VI. Privacidad por diseño y por defecto.
- Se incorpora la obligación del responsable de considerar la privacidad por diseño para cumplir con los principios del tratamiento de datos y los derechos de los titulares.
- Adicionalmente, considera que los sistemas deberán tratar por defecto sólo los datos necesarios para los fines específicos y determinados del tratamiento, así como para la extensión del tratamiento, al plazo de conservación de los datos y a su accesibilidad.

VII. Operaciones especiales de tratamiento de datos.
- Cesión. Se agrega que los datos personales podrán ser cedidos, sin el consentimiento del titular, cuando la cesión sea para el cumplimiento de un contrato en que es parte el titular.
- Mandatario. Se precisa está prohibido que el mandatario ceda los datos sin estar autorizado expresa y específicamente por el responsable para cumplir el objeto del encargo. La sanción es que se le considerará como responsable del tratamiento y responder solidariamente sin perjuicio de las responsabilidades contractuales con el mandante. Se agrega que el mandatario no podrá delegar el encargo, salvo que haya una autorización específica y por escrito del responsable. Finalmente, se establece que el mandatario debe cumplir con las normas sobre el principio de seguridad, tal como si fuera responsable, y tiene el deber de reportar directamente al responsable cualquier incidente de seguridad y a la autoridad de protección de datos si afecta a datos sensibles, de menores o de obligaciones económicas.
- Intermediarios. Se traspasa a un artículo nuevo, de manera que quede claro que se trata de un régimen diferente al de los mandatarios.
- Grandes volúmenes de datos. Se precisa que el tratamiento de esta clase debe guardar relación con las finalidades autorizadas por los titulares. Asimismo, indica que para poder hacer el tratamiento se debe tener alguna de las fuentes de licitud del

tratamiento y los titulares tienen especialmente el derecho de oposición a valoraciones personales automatizadas.

- Datos biométricos. Se precisa que además del deber de información sobre los sistemas utilizados, los datos sólo pueden ser tratados cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente.

VIII. Régimen sancionatorio.

- Se precisa que es infracción grave tratar los datos sin fuente de licitud.
- Se precisa que es infracción grave comunicar o ceder datos personales, sin el consentimiento del titular, en los casos en que dicho consentimiento sea necesario, o comunicar o ceder los datos para un fin distinto del autorizado.
- Se precisa que es infracción grave tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento, salvo que la actualización de estos datos corresponda al titular en virtud de la ley o el contrato.
- Se modifica la estructura de las multas.

Infracción	Proyecto Inicial	Comisión Constitución
Leve	Amonestación escrita o multa de 1 a 50 UTM	Amonestación escrita o multa de 1 a 100 UTM
Grave	51 a 500 UTM	101 a 1.000 UTM
Gravísima	501 a 5.000 UTM	1001 a 10.000 UTM

- Para considerar la reincidencia se baja de 30 a 24 meses.
- Los modelos de prevención de infracciones operan como atenuantes de responsabilidad.
- El plazo de prescripción de las infracciones pasa de 3 a 4 años.

IX. Modelos de prevención de infracciones.

- Se establece que los responsables pueden adoptar voluntariamente un modelo de prevención de infracciones, sea:
    - A través de la designación de un encargado de prevención o delegado de protección de datos.
    - Adopción de un modelo de cumplimiento o prevención de infracciones.
- Se regula el encargado de prevención o delegado de protección de datos, señalándose el mecanismo de designación y las funciones.
- Se regula el contenido mínimo que tienen que tener los modelos de cumplimiento o prevención de infracciones.
- Se establece que la certificación de los modelos de prevención de infracciones durará 3 años y se regirán por un Reglamento dictado por Segpres y Economía.