

PROYECTO DE LEY, EN TRÁMITE DE COMISIÓN MIXTA, QUE ESTABLECE MEDIDAS PARA INCENTIVAR LA PROTECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES (BOLETÍN N° 12.409-03)

Lorena Donoso Abarca¹

1.- Nuestra comprensión del proyecto de ley:

El Proyecto de ley es necesario en cuanto busca mejorar los mecanismos de protección de los consumidores. Dentro de los aspectos que nos interesan y a los que nos referiremos, se encuentra la referida al tratamiento de datos personales en el marco de las actividades de consumo.

2.- El derecho a la protección de datos personales.

Cuando nos referimos a “protección de datos personales”, hacemos mención a las normas dictadas para proteger los distintos derechos de las personas frente a las actividades de tratamiento de su información por parte de terceros. De manera errada hay quienes confunden protección de datos y protección de la vida privada, en circunstancias que este derecho se refiere a todo tipo de información, relativa a una persona determinada o determinable y, por ende genera una esfera de protección integral de los derechos y no sólo aquellos derivados de la privacidad.

En esos términos, la protección de datos no es susceptible de ser clasificada ni como igualdad ni como libertad, sino que se trata de un derecho habilitante. Gracias a que la persona puede controlar el uso que terceros hacen de su información, las libertades e igualdades podrán resguardarse de mejor forma.

En general se habla de datos simplemente personales y datos sensible. Mientras los datos personales son toda información relativa a personas determinadas o determinables, los datos sensibles incluyen a aquel subconjunto de datos personales cuyo tratamiento por terceros conlleva riesgos de discriminaciones.

Esto explica que información eminentemente pública como la afiliación sindical sea considerada dato sensible, pese a que es pública.

En esta comprensión, el derecho garantizado en el número 4 del artículo 19 de la constitución vigente contempla tres garantías diferentes: a) la protección de la vida privada; b) la honra de las personas; c) la protección de los derechos de las personas frente al tratamiento de sus datos personales.

Los datos personales que se tratan en el ámbito del consumo revelan los hábitos de la persona, pero también importante información sobre su situación financiera, su comportamiento de pago, por eso son tan apetecidos por la industria y comercio y tan resguardados por quienes tienen acceso a esta información.

¹ Abogado, Licenciada en ciencias jurídicas y sociales de la Universidad de Chile. Magister en Informática y Derecho y Diploma de estudios avanzados por la Universidad Complutense de Madrid, Candidata a doctor en Derecho por la Universidad de Salamanca

Una forma de acceder a más y mejor información consiste en los complejos sistemas de fidelización, que incluyen los descuentos por uso de determinados medios de pago, los sistemas de “puntos” la aceptación de inclusión en listas para recepción de ofertas, entre otros.

En esta minuta nos referiremos a los aspectos relativos al tratamiento de datos personales que se incluyen en el proyecto de ley en análisis.

3.- Los estándares internacionales en materia de protección de datos.

Dada la irrupción de las redes de comunicaciones electrónicas en todos los ámbitos de la vida de las personas, entre los cuales el consumo no es la excepción, se ha verificado una suerte de desmaterialización de las fronteras, en el sentido que las relaciones jurídicas y sociales se realizan en las redes con independencia del país en que viva o al que pertenezca una de las partes.

Por ello ha sido necesario generar estándares normativos que permitan otorgar certeza jurídica a las partes en el sentido que al menos existen mínimos comunes entre los sistemas normativos de los países. En efecto, el consumidor chileno podrá comprar en una tienda situada en cualquier parte del globo y los proveedores nacionales asimismo podrán ofrecer sus productos a consumidores ubicados en cualquier parte del planeta y ello impone desafíos adicionales al legislador.

En materia de protección de datos estos estándares se han ido construyendo a través de diversos instrumentos normativos, de los cuales destacaremos la Resolución de Madrid², que incluye aquellos mínimos que definieron los representantes de las autoridades de control de Iberoamérica, los Estándares de la OECD³, y los elaborados en el seno de la OEA⁴, por mencionar algunos de los más reconocidos.

En el plano normativo, el Reglamento de Protección de Datos de Europa⁵ sintetiza el estado del arte y se ha constituido en un estándar internacional por la vía de los hechos, al considerar en sus normas, que rige respecto de todo tratamiento de datos de los habitantes de Europa, con independencia del país en el cual se lleve a cabo.

Dentro de los estándares relevantes a nuestros efectos destacaremos los siguientes:

- a) **Principio de lealtad y licitud.** Los datos personales deben obtenerse y tratarse de forma leal y legítima. De este principio emanarán exigencias tales como la de recabar el **consentimiento** del afectado por el tratamiento de datos en aquellos casos que se exija, **la transparencia** que tiene dos aristas: **el deber de información** que implica que la persona pueda conocer qué datos se tratan respecto de su persona, a quienes se comunica la información, cuanto tiempo se mantendrán los datos (retención). Asimismo, en virtud de la transparencia, el responsable del tratamiento debiera ser capaz de explicar las reglas de negocio del tratamiento de datos y los factores de

² https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

³ [Resumen \(oec <https://www.oecd.org/sti/ieconomy/15590267.pdf>\)](https://www.oecd.org/sti/ieconomy/15590267.pdf)

⁴ [OEA :: SAJ :: DDI :: Protección de Datos Personales \(oas.org\)](https://www.oas.org/saj/ddi/proteccion-de-datos-personales)

⁵ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

cálculo que se emplean en los algoritmos tanto de recogida, como de tratamiento y comunicación de resultados del tratamiento.

- b) **Principio de finalidad.** Los datos personales sólo pueden tratarse para finalidades determinadas y no pueden ser utilizados para fines diferentes a los que fueron recabados; cumplida su finalidad deben eliminarse. De este principio emanan exigencias tales como la *'especificación del propósito'*:
- c) **Principio de necesidad o proporcionalidad.** Los datos a tratar deben ser adecuados, pertinentes y no excesivos en relación con los fines. De este principio emanan condiciones tales como la *limitación de recogida o minimización de datos, limitación de uso, temporalidad del tratamiento.*
- d) **Principio de calidad.** Quienes realicen operaciones de tratamiento de datos son responsables de que estos sean exactos y que estén al día.
- e) **Principio de seguridad.** Deben tomarse todas las providencias necesarias para evitar la destrucción accidental o no autorizada, la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados de los datos personales. De este principio se desprenden imperativos tales como los siguientes imperativos: 'responsabilidad proactiva', 'responsabilidad demostrada', 'protección de datos desde el diseño', y 'gestión de riesgos', y, en lo que nos interesa, la **'salvaguarda de seguridad'** que impone adoptar las medidas razonables para proteger los datos personales contra riesgos tales como pérdidas, accesos o usos no autorizados, destrucción, modificación o divulgación de los mismos.
- f) **Tutela efectiva del derecho:** En este ámbito se busca que exista una institucionalidad adecuada, una vía de persecución de responsabilidades efectiva y un régimen infraccional que permita perseguir las responsabilidades por las trasgresiones a los límites al tratamiento y reparación de los daños que se generen con ocasión del tratamiento de datos personales.

4.- Requisitos de una institucionalidad adecuada

El estándar señala que la institucionalidad de protección de datos debiera ser **"general"** en el sentido que se ocupe de todos los tratamientos de datos personales, con independencia de la finalidad, y la naturaleza pública o privada del responsable del tratamiento. Ello es esencial para los efectos de la seguridad jurídica y la certeza en la aplicación práctica de los criterios que se adopten.

Adicionalmente se debe tratar de una autoridad **técnica e independiente**. Técnica y profesional porque deberá resguardar los derechos de las personas frente a actividades de tratamiento de datos, que se llevan a cabo a través de complejos mecanismos tecnológicos que la autoridad debe ser capaz de comprender, interpretar, analizar y juzgar. Como regla general se ha demostrado que las autoridades meramente políticas no han resultado eficientes desde el punto de vista de la protección de los derechos o se han visto atrapadas por conflictos de intereses que en definitiva terminan poniendo en riesgos los derechos de las personas. A vía ejemplar, el Consejo para la Transparencia en Chile ha dictado múltiples resoluciones en el procedimiento de amparo que han derivado en revelación de información sensible. Es el caso

de la reciente obligación a la entrega de los datos de teléfonos de suscriptores para empresas de encuestas, la entrega de los datos del padrón electoral, otrora resuelta y la entrega de los titulares de los nombres de dominio en poder de Nic Chile, por mencionar algunos casos que resultan preocupantes. Siendo así un órgano político, dependiente del poder de turno se encuentra lejos de ser una opción aceptable.

Ello nos lleva al segundo punto de este requisito. **La autonomía** dice relación con la necesaria independencia respecto de los poderes políticos y económicos, a quienes deberán controlar, fiscalizar y eventualmente sancionar. Tanto ha sido relevado este requisito, que hay países en los cuales se establecen prohibiciones temporales de prestar servicios para instituciones controladas una vez que una autoridad de control cesa en el cargo. A vía ejemplar, el caso de España.

Adicionalmente, las autoridades de control se vincularán con las de otros países para llevar actividades de control y coordinación que se condigan con la naturaleza global de la red y el carácter transnacional de las operaciones de tratamiento de datos personales. Ello permite perfeccionar los estándares y mejorar los mecanismos de respuesta coordinada frente a quiebres de seguridad de datos.

5.- Sobre la norma propuesta.-

Las normas que se analizan tienen el mérito de responder a los imperativos y principios de tratamiento de datos personales, sin embargo yerran en al menos tres aspectos:

a.- En relación al carácter general y supletorio de la protección de datos personales como garantía de un marco de resguardo del conjunto de derechos de las personas:

En el inciso primero del art. 15 bis propuesto: La referencia a que las normas relativas al tratamiento de datos personales de los consumidores se considerarán normas especiales de protección de derechos a los efectos del artículo 2 bis y 58 de la ley 19.496 carece de utilidad práctica, pues esas normas hoy ya se consideran datos personales, con aplicación general y por tanto también al consumo, sin necesidad de modificación legal. Es más la aprobación de esta parte podría traer aparejado luego problemas de interpretación.

Sería más relevante si se agregara a la “información básica comercial” la información relativa a las políticas de tratamiento de datos personales o “políticas de privacidad” en los sitios de las compañías.

Adicionalmente, las reglas de tratamiento de información comercial se encuentran reguladas en el artículo 37 que por efectos del proyecto pasa a ser 20.

b.- En relación al principio de calidad y seguridad del tratamiento de datos personales.

En el inciso segundo del art. 15 bis propuesto: La norma induce a equívocos porque el sujeto obligado es el proveedor, quien hoy en día ya está obligado por la ley 19.628, sin necesidad de esta nueva norma legal. Asimismo, al referirse solo a los datos personales del inciso anterior, restringe los derechos de las personas y genera problemas de interpretación.

Adicionalmente, la norma parece restringir los derechos y las reglas de protección de datos al deber de reserva y secreto y la finalidad del tratamiento, dejando de lado los demás principios y normas de tratamiento de datos personales.

Asimismo, la norma olvida referirse a la ley 20.575, lo cual es un error desde la óptica sustantiva y genera fragmentación del sistema jurídico.

c.- En relación al principio de control y tutela efectiva del derecho.

En materia de la institucionalidad del texto propuesto se desprende que las violaciones de seguridad debieran informarse al Servicio Nacional del Consumidor, lo cual genera una mayor dispersión normativa de la que ya existe en nuestro país, en el plano institucional, con la consecuente afectación a la seguridad jurídica y en cuanto a que la autoridad a la cual debieran comunicarse los datos a que se refiere no es autónoma en los términos requeridos en la legislación de protección de datos personales.

d.- En relación a la prohibición de realizar descuentos asociados a un medio de pago.

La modificación no parece ser necesaria, por cuanto el texto actualmente vigente incluye la prohibición de realizar ventas atadas, de incurrir en discriminaciones arbitrarias, las cuales son de carácter general para todos los proveedores de productos financieros.

En caso de estimarse necesario reforzar estos aspectos, podría incluirse la obligación de informar a los consumidores de manera clara y transparente sobre las condiciones de los descuentos aplicados y el destino de los datos personales que se recogen con ocasión del aprovechamiento de las ofertas de parte de los consumidores y usuarios.

Al respecto, es importante atender al principio de equivalencia normativa, siguiendo en estos aspectos la experiencia de los mercados de referencia, sobre todo considerando el carácter transnacional del comercio electrónico.

Propuesta.-

- a) Mantener el artículo en su texto aprobado en la cámara de diputados.
- b) En caso que se estime necesario perseverar en la modificación, incluir los aspectos sustantivos de la propuesta del senado, en los siguientes aspectos:
 - a. Incluir los plazos de información a los consumidores de la violación de seguridad
 - b. Incluir la plena vigencia en materia de consumo de los principios y derechos de protección de datos personales.
- c) En materia de institucionalidad, incluir que los reclamos de las personas en estas materias se tramitarán de acuerdo a las reglas del ejercicio de derechos en materia de protección de datos (derecho de acceso)