
Minuta

Proyecto de Ley de Reforma de Ley 19.628 sobre Protección de la Vida Privada (Boletín 11.144-07 y 11.092-07 refundido)

I. Comentarios Generales.

Desde la Cámara Nacional de Comercio (CNC), creemos que Chile cuenta con la oportunidad de contar con un marco de protección de datos personales que proteja la privacidad y a la vez que facilite los usos beneficiosos e innovadores de los datos en un entorno de negocios y tecnológico en constante evolución, lo cual en última instancia garantizará la competitividad económica del país.

No obstante lo anterior, esta oportunidad de mejorar nuestros estándares de protección, no debe implicar una sobre regulación, que se traduzca en aumentos en las estructuras de costos, especialmente para la pequeña y mediana empresa, haciéndolas menos competitivas en relación al resto de las empresas no solo a nivel local sino también a nivel mundial.

Así las cosas, el texto del proyecto logra a nuestro entender, un equilibrio entre la protección de la privacidad de los ciudadanos y la circulación de la información como motor fundamental del desarrollo de la economía digital.

Sin embargo, como CNC, recomendamos que en esta nueva normativa: **(a)** siga los principios de la OECD, organismo del cual Chile es parte y no de normativa de tratados, en los cuales Chile no es parte como la Unión Europea; y **(b)** no se discrimine respecto de ninguna industria.

II. Comentarios específicos.

1. CONSENTIMIENTO. ARTÍCULO 12 INCISO 6 DEL PROYECTO DE LEY.

Señala el artículo 12 inciso 6 del Proyecto de Ley que *“El consentimiento no se considerará una base jurídica suficiente para la validez del tratamiento de datos, cuando exista un desequilibrio ostensible entre la posición del titular y el responsable”*.

Comentarios. Esta disposición no se encuentra en el derecho comparado, ni en el Reglamento de Datos Personales de la Unión Europea (el “Reglamento”). El Reglamento, en su considerando 43, se refiere a la situación de *“desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.”* Sin embargo, el Reglamento opta por no incluirlo como una disposición prescriptiva, sino que hacer mención de esta situación en los considerandos, en relación con autoridades públicas. Una disposición como la señalada, pone en riesgo la seguridad jurídica de todo el proyecto de ley y lo afecta seriamente.

Además de lo anterior, la necesidad de calificar un *“desequilibrio ostensible”* llevará a la autoridad administrativa o judicial a tener que pre-definir escenarios de desequilibrio que pueden encontrarse alejados de la realidad (por ejemplo, la aceptación de una política de privacidad a través de un checkbox online, que es la forma que opera todo el comercio electrónico internacional, quedará proscrita per-se pues se considera que existe un desequilibrio ostensible).

El problema del *“desequilibrio ostensible”* ya ha sido resuelto tanto por el derecho comparado como por el derecho nacional, el primero: (1) generando obligaciones de publicidad y transparencia respecto de la política de privacidad vigente, la que debe ser redactada en forma clara y estar siempre disponible para el titular de los

datos; y (2) facilitando las herramientas del titular en torno a sus derechos fundamentales como el acceso y la rectificación; mientras que el derecho nacional a través del artículo 1451 del Código Civil y siguientes correspondiente a los vicios de la voluntad (error, fuerza y dolo). Asimismo, se propone que al igual que lo señalado en el texto de la moción de senadores (Boletín 11.092-07) y la intención del Ejecutivo durante la discusión legislativa sobre este punto, se regule el consentimiento para el tratamiento de datos personales, no condicionándolo a la ejecución de un contrato y/o a la prestación de un servicio.

Propuesta de Modificación.

En vez de utilizar el concepto de “desequilibrio ostensible”, evitar ciertas situaciones en las que claramente sí habría un desequilibrio. Así, se podría avanzar en un inciso 6 en el siguiente tenor, de acuerdo al considerando 43 del reglamento:

Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. De esta forma, al evaluar si el consentimiento se ha dado libremente, se tendrá en consideración el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento el tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

TAMBIÉN PODEMOS COMBINARLO CON EL ARTÍCULO 16 LETRA G) DE LA LPDC

2. INTERMEDIARIOS TRATAMIENTO DATOS PERSONALES. Artículo 15 BIS INCISO 6 DEL PROYECTO DE LEY.

Señala el Artículo 15 bis inciso 6 del Proyecto de Ley que “*Las personas naturales o jurídicas que presten servicios de infraestructura, plataforma, software u otros servicios para el almacenamiento o procesamiento de los datos, o para facilitar enlaces o instrumentos de búsqueda, no tendrán la calidad de responsable de datos para los efectos de esta ley, salvo que tomen decisiones acerca de los medios y fines del tratamiento de datos, en cuyo caso responderán de acuerdo a las normas previstas en esta ley para los responsables de datos, sin perjuicio de las demás responsabilidades y sanciones que les puedan caber por incumplimiento de contratos o infracciones legales*”.

Comentarios. Esta disposición hace referencia a la figura de intermediarios, que debe distinguirse claramente de la de responsable, ya que tienen naturaleza diferente.

Propuesta de modificación.

Debiera dejarse establecido fehacientemente que se trata de personas que no tienen el control de los datos respecto de los cuales se utilizan sus servicios y en consideración a lo mismo responden únicamente de aquellos tratamientos específicos respecto de los cuales sí tomaron decisiones respecto de medios o finalidad.

3. PLAZOS PARA CALIFICAR REINCIDENCIA Y PARA APLICAR SANCIÓN DE SUSPENSIÓN DE OPERACIONES. Artículos 40 y 42 DEL PROYECTO DE LEY.

Comentarios. En el artículo 40 del Proyecto se señala que:

“Se considerarán circunstancias agravantes: a) La reincidencia. Existe reincidencia cuando el responsable ha sido sancionado en dos o más ocasiones, en los últimos treinta meses, por infracción a esta ley. Las resoluciones que aplican las sanciones respectivas deberán encontrarse firme o ejecutoriadas.”

Sin embargo, en el artículo 42 se establece la “*Sanción de suspensión de las operaciones y actividades de tratamiento de datos por hasta 30 días en caso de reincidencia de infracciones gravísimas reiteradas en un período de 24 meses*”.

Se recomienda equilibrar los dos plazos, bajando de 30 meses a 24 meses, el plazo dentro del cual, cuando se comete una infracción, se califica la reincidencia en el artículo 40.

Propuesta de Modificación.

Es por lo anterior que se propone equilibrar el plazo en 24 meses, como también lo hace la LPDC en su última reforma pronta a ser promulgada.

4. OBLIGACIONES DE REPORTE DE BRECHAS DE SEGURIDAD DE LOS MANDATARIOS O ENCARGADOS. Artículo 15 bis inciso 4° DEL PROYECTO DE LEY.

Comentarios. El artículo 15 bis, que regula el tratamiento de datos a través de mandatario o encargado, establece en su inciso cuarto que “*El tercero mandatario o encargado deberá cumplir con lo dispuesto en los artículos 14 bis, 14 quater y 14 quinquies.*”

Proponemos la eliminación de la referencia al artículo 14 quinquies, que se refiere a las obligaciones de reporte de brechas de seguridad.

Un encargado del tratamiento no puede estar obligado a reportar una brecha de la misma forma, en iguales plazos y al mismo nivel que el responsable, pues:

(i) La calificación de brecha de seguridad, para efectos de su notificación, debe hacerla sólo el responsable: La notificación a la autoridad en el escenario del inciso primero del artículo 14 quinquies involucra una calificación de la ocurrencia de la brecha, es decir, el obligado debe evaluar si la vulneración a la seguridad efectivamente ocasiona las consecuencias allí previstas (destrucción, alteración, etc.) sobre datos los personales que trata. En muchas ocasiones, un encargado no tiene siquiera acceso al contenido de lo procesado, por lo que no está en posición de evaluar las consecuencias de la brecha respecto de los datos que trata. Incluso si tuviera acceso al contenido de lo procesado, la existencia de dos obligados a calificar la brecha y notificar permite obvias contradicciones. Quien debe hacer esa evaluación (que es una evaluación tremendamente delicada para un negocio) y decidir finalmente el hecho de la notificación a la autoridad, es el responsable. Por esa razón es que el propio GDPR (General Data Protection Regulation de Europa) establece que el encargado debe notificar al responsable, y no a la autoridad. Es el responsable quien tiene la obligación de notificar a la autoridad.

(ii) Similar situación sucede con la obligación de notificar a los titulares de datos, bajo el inciso final del artículo 14 quinquies: estando el responsable y el encargado igualmente obligados a notificar a los titulares, la calificación de la gravedad que involucra esa notificación no pueden hacerla dos personas, y no puede hacerla una persona diferente del responsable, quien está en mejor posición de calificar el impacto.

Un encargado cumple un rol técnico y, por definición, neutro. Si bien es de toda lógica que puede ser objeto de una brecha de seguridad al mismo nivel que un responsable, su obligación debe ceñirse a notificar a los responsables de la ocurrencia de esa brecha.

El GDPR establece en su artículo 28 letra (f) una obligación para el encargado de asistir al responsable en el cumplimiento de las obligaciones de seguridad; pero el sujeto obligado respecto de estas es únicamente el responsable. En ese sentido no tiene el encargado una obligación activa de reportar a la autoridad o a los titulares, la ocurrencia de brechas de seguridad.

Propuesta de Modificación.

Es por lo anterior que se propone eliminar la referencia al artículo 14 quinquies del artículo en análisis..
