Modifica la ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores, en el sentido de imponer a los proveedores que indica, la obligación de dar a conocer las vulneraciones a las bases de datos que contengan información sobre sus clientes o usuarios

Boletín N°12099-03

I.- ANTECEDENTES.

A nuestro país le queda un largo camino por recorrer para que podamos alcanzar estándares adecuados y pertinentes que garanticen nuestra defensa nacional en materia de ciberseguridad y podamos convivir en una sociedad digital segura, en donde todos podamos disfrutar los beneficios que las nuevas tecnologías nos proveen.

La Unión Internacional de Telecomunicaciones, organismo especializado de la Organización de las Naciones Unidas para las tecnologías de la información y la comunicación, define la "*ciberseguridad*" en la Recomendación **UIT-T X.12052**, que luego fue aprobada con la Resolución N° 1813, y señala que "*La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios y los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedias, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad*".

En tal sentido, debemos asociar la ciberseguridad como una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como aquel conjunto de infraestructuras físicas, lógicas y las interacciones humanas que ahí convergen. Donde los aspectos esenciales a resguardar se enmarcan en la confidencialidad, integridad y disponibilidad de la información.

Este problema, a nuestro juicio, requiere - al menos - contar con respuestas institucionales por un lado, y jurídicas por el otro. A nivel institucional, no contamos actualmente en nuestra estructura estatal con instituciones especializadas que tengan por objeto prevenir u alertar previamente estos ataques. Tampoco contamos con instituciones que gestionen, una vez ocurridos estos ciberataques, los efectos o consecuencias que puedan producir en la población, que determinen su origen, que establezcan la identidad de los responsables y que recomiende medidas que tiendan a perfeccionar nuestra defensa en esta materia. Lo que no es menor, si consideramos que las transacciones de "e-commerce" en nuestro país siguen aumentando explosivamente, las que llegarían en 2018 a los US$5.000 millones y al año 2020 superarían los US$8.000 millones en ventas (según datos de la Cámara de Comercio de Santiago).

Por otro lado, requerimos de respuestas a nivel jurídico, requiriendo un estatuto especial que se haga cargo de esta particular materia y sus diversos fenómenos, tan relevantes para el siglo XXI y que se caracteriza por la reducida información que controlamos, ya que la internet que conocemos solo representa 4% de todo el tráfico web del mundo, pues el 96 % restante se encuentra en la web profunda o "deep web". Lugar donde generalmente operan los *hackers* que perpetran los ciberataques y donde transan la información que recolectan fraudulentamente de las bases de datos que cuentan con información de los usuarios. Espacio que, sin un monitoreo pertinente y las medidas de seguridad adecuadas, nos deja en la más absoluta indefensión o peor aún como un objetivo recurrente de estos perpetradores informáticos.

Actualmente Chile solo destina 0,07 del PIB nacional en ciberseguridad, cifra que si bien ha aumentado en los últimos años (pasando en el año 2016 de US $187 millones a US $195 millones en el año 2017), nos sitúa muy por debajo del promedio mundial que destina alrededor de 0,12% del PIB para estas materias. Frente a ello, debemos poner todos nuestros esfuerzos para sentar las bases que nos permitirán lograr una sociedad digital segura y promover la inversión necesaria que nos permita concretarla.

En este sentido, en el mes de junio del 2018, el Superintendente de Banco e Instituciones financieras se reunió con gerentes generales de los bancos Santander, de Chile, Estado, BCI, Itaú, Scotiabank, Falabella, Ripley, BBVA, Bice y Security, a fin de hacerles ver que debían tomar medidas adicionales a las vigentes, en vista y considerando que "para este año la banca está desembolsando $ 674.304 millones en TI, lo que

representa un 8,4% respecto a los resultados operacionales de la banca y significa un crecimiento de 46,8% respecto de 2015. Mientras que para ciberseguridad, la banca está invirtiendo este año $ 60.961 millones, lo que equivale solo al 8,2% del total destinado a TI. Además, dicho monto equivale al 0,8% de los resultados operacionales brutos del sistema"[1] .

Sin embargo, en los últimos años, principalmente durante en lo que va del año 2018, hemos sido testigos de lo frágil que es nuestro sistema de ciberseguridad y el grave riesgo que corre nuestra información en manos de particulares, que día a día suministramos a los distintos proveedores de servicios. Esta situación no afecta exclusivamente a la prestación de servicios financieros, sino que a la totalidad de prestadores de servicios que cuentan en sus bases de datos con información de sus clientes o usuarios, siendo los más relevantes el área de la salud y el comercio. Respecto de este último, según el 11° Informe Anual de Ciberseguridad (ACR) de Cisco 2018, en el año 2017 se reportaron 1.093 brechas de seguridad a nivel mundial, un 40% más que el año anterior. "*Eso significa que de cada tres retailers, uno de ellos fue víctima de un ciberataque, lo que se traduce en un 20% en pérdidas de clientes*". Por eso la ciberseguridad debe ser relevante al momento de pensar en la transformación digital.[2]

A raíz de estas vulneraciones, hemos tomado conciencia que las vulneraciones de bases de datos con información de los consumidores en manos de proveedores de servicios (financieros o no), solo han salido a la luz y se han dado a conocer a la opinión pública a través de los distintos medios de comunicación por filtraciones o lo que es peor, por comunicados en que los mismos hackers se atribuyen su responsabilidad junto a la divulgación masiva de la información obtenida a partir del ciberataque.

Esta situación resulta de la más extrema gravedad, ya que solo estas instancias nos permiten percatarnos de los ciberataques que sufren los consumidores, a diferencia de lo que ocurre en el derecho comparado donde, por ejemplo, a través del Reglamento de Protección de Datos de la Unión Europea o la legislación que regula los grandes mercados financieros, como Nueva York o Londes, las entidades se encuentran obligadas a reportar la vulneración a la autoridad competente. En Chile, muy por el contrario, depende de cada empresa y sus normas de cumplimiento la decisión de informar o no estos

[1] Vera, Vicente. Bancos invierten 0,8% de sus resultados en ciberseguridad. Diario Financiero, 19 de junio 2018, p. 21.
[2] DIARIO FINANCIERO. Ciberseguridad: La clave para potenciar nuevos modelos de negocio en la era digital, 05 de abril 2018, suplemento, p. 4.

ciberataques. Existiendo mayor incentivo a mantener bajo reserva estas situaciones, dados los efectos negativos que reportan a la empresa como el prestigio de la marca, fuga de clientes, la reacción de los "*stakeholders*", la valorización misma de la empresa, entre otros. Sin embargo, esta conducta es dañina ya que no soluciona el problema de fondo (pudiendo ser afectados nuevamente) y desincentiva la inversión en ciberseguridad, al poner sus esfuerzos en la sola contención de la noticia que en la prevención de estos hechos.

II.- IDEA MATRIZ

Por estas consideraciones, la presente iniciativa pretende establecer la obligación de los proveedores que tengan en sus bases de datos información de sus clientes y las operaciones que estos efectúen, de informar al Servicio Nacional del Consumidor y a sus clientes, de todo ataque o vulneración de seguridad de que sean objeto sus bases de datos que contengan la información de sus cliente, sus registros y operaciones de toda índole.

III.- CONTENIDO DE LA INICIATIVA LEGAL.

El Proyecto de ley pretende modificar la ley N°19.496, que Establece Normas Sobre Protección de los Derechos de los Consumidores, creando un artículo art. 14 bis, bajo el titulo II, párrafo 3, que establece las obligaciones de los proveedores frente a los consumidores, extendiendo el deber de informar al Servicio Nacional del Consumidor y a los consumidores afectados por las vulneraciones a las bases de datos que cuenten con información de los consumidores.

Frente a la infracción de esta obligación, se establece como sanción la misma que se prescribe para las conductas consistentes en publicidad falsa o engañosa engañosa, contenida en el inciso segundo, articulo 24 del mismo cuerpo legal, esto es, con multas de hasta 750 UTM.

PROYECTO DE LEY

"ARTTICULO UNICO. Incorpórese un nuevo artículo 14 bis, en la ley N° 19.496, que "Establece Normas sobre Protección de los Derechos de los Consumidores", del siguiente tenor:

Artículo 14 bis. Los proveedores, que efectúen el tratamiento de datos personales o comerciales de los consumidores y sus operaciones, tendrán la obligación de informar al Servicio Nacional del Consumidor y a los consumidores afectados, todo tipo de violación de seguridad que afectaren sus bases de datos o de las que se sirvan y que contengan

información de sus clientes o usuarios, sin dilación indebida y desde el momento en que hayan tomado conocimiento del hecho.

La comunicación de estos hechos deberá efectuarse a través de cualquier medio físico o digital que resulte más idóneo y que garantice su celeridad. Si el proveedor cuenta con servicio de atención a los clientes, dispondrá y canalizaran a través de estos servicios las consultas y reclamos de los consumidores afectados.

La infracción a esta obligación, se sancionará con multa de hasta 750 Unidades Tributarias Mensuales. En caso de demora o dilación indebida se sancionará al proveedor con multa de hasta 1.000 Unidades Tributarias Mensuales.”