FJG

FUNDACIÓN JAIME GUZMÁN

DESAFÍOS DE LA CIBERSEGURIDAD

N° 254 | 29 de agosto 2018

Ideas & Propuestas

RESUMEN EJECUTIVO

La ciberseguridad se ha convertido en un tema fundamental que demanda desafíos a todos los países. Los ataques que han sufrido algunos bancos recientemente en Chile obligaron al gobierno a revisar nuestra legislación al respecto. La siguiente edición de “Ideas & Propuestas” tiene como objetivo una revisión sobre los casos acontecidos al país en materia de ciberseguridad, junto con una proyección a cuál debe ser el rol del Estado en la materia.

Foto: t13.cl

I. INTRODUCCIÓN

Mientras más progresan las comunicaciones y el desarrollo informático-digital, mayores son los desafíos para la protección de la vida privada. Resulta necesario entonces profundizar el procesos de comprensión de los retos que significan avanzar en formas modernas de regulación que impliquen interpretar una sociedad cada vez más digitalizada, las cuales proyectan nuevas formas de comunicación social.

Nuestro país ha demostrado poseer una institucionalidad sólida en múltiples dimensiones, sin embargo, al parecer los últimos eventos vinculados a la ciberseguridad que han afectado directamente al Banco de Chile han sido una señal de alerta para el mundo político, académico y comercial. Desde el robo de US$ 10 millones desde Hong Kong, la filtración de 14 mil tarjetas de crédito tras otro ataque cibernético, el robo de más de 400 millones de pesos por un profesional especialista en operaciones y, ahora último, la reciente filtración de 916 tarjetas de crédito, han generado más que una alerta.

Algo está pasando en nuestro país en materia de ciberseguridad y si bien la banca ha sido la más afectada a nivel público, las implicancias del desarrollo de políticas públicas en torno a este tema no pueden acotarse al mundo bancario.

La ciberseguridad abarca diversas dimensiones de elementos desarrollados a través de soportes informáticos, por lo tanto está directamente relacionada a otros sectores del desarrollo productivo de nuestro país, como la industria aeronáutica y portuaria, entre otras. Es por ello que a raíz de toda la discusión pública que se ha suscitado, el Gobierno y la oposición han dado señales de avanzar en una nueva regulación que pueda estar acorde a los desafíos actuales.

II. CASO BANCO DE CHILE: UNA CRISIS DE LA INFORMACIÓN

Tal vez el caso más emblemático en la materia es el ciberataque perpetrado por hackers internacionales al Banco de Chile. El pasado 24 de mayo del año 2018, la compañía fue atacada por un virus que ingresó a sus sistemas y generó el robo de US$10 millones mediante 4 transacciones del sistema Swift[1] que lograron concretar el hackeo. Cada transacción llegó a una cuenta distinta de Hong Kong. Durante los días posteriores el ilícito fue vinculado a Lazarous Group, entidad proveniente de Norcorea, quienes habrían traspasado el monto al gigante chino.

El día 31 de mayo el Banco de Chile reportó la situación a la policía de Hong Kong y el 18 de julio un equipo de investigación de Hong Kong arrestó a un hombre chino de 28 años por el delito de "tratar con propiedad que se sabe o se cree que representa el producto de un delito procesable", lo que en palabras de Pulso constituye "lavado de dinero"[2].

Anteriormente, el 25 de junio, la entidad controlada por el Grupo Luksic y Citibank presentó una demanda ante la corte de primera instancia del Tribunal Superior de Hong Kong, conocida como High Court. El objetivo era exigir la devolución de US$5.488.590 que llegaron a una cuenta perteneciente a Ketuo Trade Limited. Esta firma está inscrita en el registro de compañías de Hong Kong en marzo de 2017 bajo la etiqueta de "empresa privada limitada por acciones", con oficina en el Ho King Commercial Centre, un centro comercial de Hong Kong.

Posteriormente, el 12 de julio, la firma presentó otra acción ante el mismo tribunal, pero esta vez contra Boruida Trading Co Limited, Tech Giant Limited, y Minerva Holding Limited, las que serían titulares de las cuentas en las que se depositaron parte del dinero sustraído al banco chileno. Cabe consignar que para todas estas acciones, el Banco de Chile fue asesorado por el estudio de abogados Linklaters, con sede en Londres, quienes también poseen oficinas en al menos 20 países, incluido Hong Kong.

Paralelo a estas acciones judiciales dirigidas por el Banco de Chile, el tema se tomó la agenda pública. El 6 de junio se realizó una sesión especial en la Comisión de Economía del Senado sobre la falla en el sistema del Banco de Chile, en la ocasión asiste el superintendente de Bancos Mario Farren. Sumado a esto el tema comenzó a escalar a nivel de reuniones entre autoridades de gobierno y reguladores.

[1] El término SWIFT deriva del inglés y traducido al español significa Sociedad para las comunicaciones Interbancarias y Financieras mundiales. Se trata de una entidad que tiene a su cargo una amplia red mundial de comunicaciones de tipo financiera entre distintas entidades bancarias o financieras.

[2] Ver más en https://bit.ly/2MkpZmQ

Finalmente, el 18 de julio la policía de Hong Kong arresta a un ciudadano de nacionalidad china.

El Gobierno chileno manifestó una inmediata preocupación de los estándares del país en la materia, el cual, especialmente en temas financieros, reveló una exposición. El mismo Presidente Sebastián Piñera hizo un llamado a evitar más hechos como este[3]. De este modo, y tras gestiones con distintas entidades (Banco Central, Comisión de Mercado financiero, Superintendencia de Bancos y Superintendencia de Pensiones) es que se generó el compromiso de trabajar por más seguridad en el sistema financiero local, identificando brechas entre estándares internacionales y nacionales, además de una revisión de la regulación en la materia que permita generar cambios necesarios para adecuar nuestra realidad al estándar internacional exigido en la materia. El mismo Superintendente de Bancos, Mario Farren, estableció que tras este ciberataque el foco de su gestión será la ciberseguridad en la industria.

Luego del ataque al Banco de Chile se diseñó un plan de acción concreto. Entre los principales ejes de acción para modernizar y perfeccionar protocolos y marco regulatorio es que se acordó contratar a un organismo internacional que preste asesoría "para identificar las brechas en relación con los estándares y recomendaciones internacionales para prevenir y enfrentar los ciberataques que pueden sufrir las entidades del mercado financiero, con especial énfasis en los bancos", según indicó Hacienda mediante un comunicado de prensa[4].

El Comité Interministerial acordó que agosto sería el plazo final para presentar propuestas de ciberseguridad con miras a una posterior legislación. En este sentido, la administración de la entonces Presidenta Michelle Bachelet, estableció 41 medidas con lineamientos políticos del Estado en la materia. El documento llevó por nombre "Política Nacional de Ciberseguridad" y contaba con una mirada que apuntó al año 2022. No obstante, de estas medidas, sólo 8 fueron cumplidas por la administración de Michelle Bachelet[5].

El Gobierno del Presidente Piñera, por su parte, prepara un proyecto que será enviado al Congreso para adecuar la normativa, la cual data del año 1993. El proyecto establece ocho conductas criminales y la captación y divulgación de imágenes obtenidas sin autorización. En este sentido los desafíos en la materia se encuentran a nivel de seguridad, reconociendo que nuestro sistema bancario es sólido, pero entendiendo a su vez que una política nacional de ciberseguridad se vincula a los más variados sectores de la economía.

[3] Ver más en https://bit.ly/2Ns0Mn6

[4] Pulso, 13 de junio de 2018. Ciberataques: Gobierno buscará asesoría internacional y apunta a coordinadar a reguladores.

[5] Íbid.

Foto: radioagricultura.cl

III. LOS DESAFÍOS DE LA CIBERSEGURIDAD

Tras los episodios relativos a la vulneración cibernética de datos confidenciales, es que el Gobierno del Presidente Sebastián Piñera decidió nombrar a Jorge Atton como asesor presidencial en ciberseguridad. Entre los desafíos de Atton está el avance y colaboración en la confección de una ley marco que regule la ciberseguridad, además de la creación de una unidad especializada en la materia, conocida como CERT (Equipo de Respuestas ante Emergencias Informáticas por sus siglas en inglés).

Nuestro país se encuentra trabajando junto a mesas de trabajo con asesores internacionales, como el Banco Interamericano de Desarrollo (BID), empresas privadas, el mundo parlamentario, ONG y universidades. Se espera que el CERT chileno pueda ser una respuesta ante la falta de respuestas ante incidentes cibernéticos. Jorge Atton y el subsecretario del Interior, Rodrigo Ubilla, iniciaron trabajos para una nueva normativa legal en materia de ciberseguridad. Para ello se reunieron con el secretario general del Instituto Nacional de Ciberseguridad de España (Incibe), Francisco Pérez Bescon la intención, según informó prensa[6], de firmar un convenio con esta entidad, que es un referente de la ciberseguridad en toda Europa.

El objetivo de esta acción radica en enviar al congreso iniciativas legislativas prioritarias, además de generar acciones vinculantes con el sector privado y la ciudadanía. La experiencia de la Unión Europea y España son claves.

Tal vez el aspecto más relevante en materia de ciberseguridad es entender que esta es un elemento central en la gestión de riesgos operacionales. Es más, es parte elemental de nuestro sistema financiero, pero abarca mucho más que la banca y el mundo bursátil;

[6] Ver más en https://bit.ly/2wvcgie

se encarga de diseñar normas para distintos sistemas de información. En esa dirección, René Leiva, en un artículo de opinión titulado "La banca es parte de la ciberinfraestructura crítica nacional" remarcó "la alta importancia que ha alcanzado el segmento del ciberespacio que ocupa la Banca como parte vital de su operación, debiendo entenderlo como una parte de la ciber infraestructura crítica nacional, cuyo daño o afección puede tener graves efectos en los intereses esenciales y la seguridad de cualquier país".

Leiva hace un llamado a generar "normativas obligatorias y no orientadores para toda la infraestructura crítica nacional, en especial a las entidades bancarias, algunas de las cuales han develado que prefieren correr el riesgo de ser vulnerables a las amenazas antes de invertir en la protección de sus activos de información".

Actualmente existen 3 proyectos fundamentales que apuntan a hacer frente a este fenómeno y que serán presentados durante el segundo semestre de este año: Modificación a la Ley de Delitos Informáticos, Ley Marco de Ciberseguridad y Ley de Infraestructura Crítica de la Información.

El pasado 13 de agosto, en sesión especial, la Sala de la Cámara de Diputados analizó las vulnerabilidades de la infraestructura estratégica del Estado ante ciberataques, además de la realidad nacional en materia de legislación informática. En la oportunidad se aprobaron distintas resoluciones, entre ellas, una que solicita al Presidente de la República trabajar concretamente una política pública de carácter nacional en materia de ciberseguridad, con el objeto de dotar a las Fuerzas Armadas de un margen de acción, tanto en la defensa, como disuasión y reacción ante eventuales amenazas contra la seguridad nacional. Por otro lado también se aprobó otra que busca promover protocolos, políticas, programas y leyes, tendientes a incrementar la seguridad virtual de los soportes electrónicos de Bancos e Instituciones Financieras.

Dicha sesión también aprobó solicitar a los ministros del Interior y de Seguridad Pública y de Defensa que adopten todas las medidas para elevar al máximo las exigencias en materia de protección cibernética en todos los asuntos de seguridad nacional.

Estos acontecimientos van en línea con una renovación del RoI del Estado en la materia generando proyectos relevantes que buscan modificar leyes que rigen desde fines de los 90 -como la modificación a la Ley 19.223- con el objetivo de facilitar la persecución de nuevas figuras penales, las cuales -dados los avances tecnológicos- llegaron para quedarse.

Por otro lado, se espera que la Ley Marco de Ciberseguridad permita crear un equipo multidisciplinario con facultades para exigir a las empresas privadas mayor compromiso incidentes informáticos. A su vez, la Ley de Infraestructura Crítica de la Información busca que nuestro país pueda otorgar penas más altas a los hackers que ataquen activos esenciales para el funcionamiento de la sociedad y la economía, elemento más conocido como "infraestructura crítica para nuestro país".

IV. CONCLUSIONES

Los recientes acontecimientos en materia de ciberseguridad revelaron una débil institucionalidad y una regulación local desactualizada. El impacto generado, no solo por el robo de millones de dólares, sino además por la filtración de la información privada relacionada a miles de tarjetas de crédito, reveló algo impensado hace años atrás: nuestro país necesita actualizar sus políticas de ciberseguridad. Estos eventos vulneraron no sólo los derechos de consumidores y usuarios, sino que dejó al desnudo las falencias en cuanto al Rol del Estado en la materia.

Vivimos tiempos donde la seguridad se convierte en un aspecto fundamental sobre el cual los gobiernos no pueden quedarse atrás. Es necesario que el Estado tenga la capacidad técnica y legal de enfrentar amenazas que puedan poner en jaque áreas sensibles de nuestra estructura, no solo económica o financiera, sino también en otras materias vinculadas a seguridad y redes. Nuestra legislación vigente data de fines del siglo XX, y según la evidencia lo demuestra, no se encontraría a la par con los desafíos contemporáneos.

Sin embargo, creemos que esto tampoco puede ser excusa para generar lógicas burocráticas que entrampen un sistema que a pesar de los recientes acontecimientos, ha demostrado estar en la primera línea de las tendencias mundiales.

En este sentido valoramos la necesidad de avanzar en los 3 proyectos que se comenzarán a discutir a partir de esta coyuntura: la Modificación a la Ley de Delitos Informáticos, la Ley Marco de Ciberseguridad, y la Ley de Infraestructura Crítica de la Información. Estas iniciativas apuntan en la dirección correcta, entregando al Gobierno los insumos necesarios para robustecer no solo nuestro sistema financiero, sino que también otras áreas sensibles de nuestro país, como son la economía y las telecomunicaciones.

Esto va más allá que un problema bancario, hablamos de leyes entienden este tema como una estrategia nacional, que incluyan, por ejemplo, cooperación público-privada y que a la vez nos permita respetar la privacidad y la libre circulación de la información, manteniendo un estándar de país OCDE.

Es necesario que nuestro país posea un marco legal capaz de hacer frente a los nuevos delitos que se están cometiendo en el mundo virtual. Los proyectos que el Gobierno va a presentar apuntan en esa línea, incorporando, no sólo nuevos delitos informáticos, sino que además aumentando la rigurosidad con el tratamiento de estos.

Capullo 2240, Providencia.

www.fjguzman.cl /FundacionJaimeGuzmanE @FundJaimeGuzman