Diario Constitucional.cl
Domingo, 9 de agosto de 2020

Artículos

Santiago, 30 de julio de 2018

Brechas de datos, a propósito de la filtración de datos de tarjetas de crédito.

Lo sucedido revela una clara deficiencia en nuestra legislación de protección de datos personales, y esta es que gran parte de la información fue primero publicada por medios de prensa, redes sociales; mientras que los bancos afectados informaron por Twitter, sus páginas web y correo a sus clientes de los ataques ocurrido

Por: Pablo Lapostol

La noche del día miércoles y sábado pasados las noticias que circularon con velocidad por la red fueron las filtraciones de datos de cuentas corrientes de clientes de bancos chilenos. "TheShadowBrokers"-un grupo de hackers- habría robado u obtenido de manera ilegal esta información, entregándola de manera pública por Internet. Los afectados, personas desprevenidas que probablemente se enteraron primero a través de redes sociales, tuvieron conocimiento de que su información se encontraba fuera del control de a quienes la habían confiado (en este caso diversos bancos).

Más allá de las medidas que puedan tomarse para enfrentar esta situación, en particular los ataques a bases de datos y robos de información, se han convertido en algo cotidiano en nuestra sociedad. Si pensamos por ejemplo en el caso de la brecha de EQUIFAX que ocurrió el año pasado -en que 145.5 millones de estadounidenses vieron su información personal robada- se hace necesario tomarnos un tiempo para reflexionar a quien confiamos nuestra información, que garantías nos otorgan de su resguardo y en caso de que fallen en resguardar nuestra información si podríamos ser informados para poder tomar las precauciones correspondientes.

Las garantías de resguardo pertenecen al ámbito de la ciberseguridad, contando este campo que en nuestro país con un desarrollo emergente . A partir de la publicación de la Política Nacional de Ciberseguridad, diversas autoridades han comenzado a emprender tareas de modernización de los estándares de protección en esta materia. Pero, ¿qué sucede cuando la seguridad falla?

Lo sucedido revela una clara deficiencia en nuestra legislación de protección de datos personales, y esta es que gran parte de la información fue primero publicada por medios de prensa, redes sociales; mientras que los bancos afectados informaron por Twitter, sus páginas web y correo a sus clientes de los ataques ocurridos. Aún quedan hechos por esclarecer en este ataque, pero ¿es esta la mejor manera en que estas instituciones pueden informar de los ataques a las personas afectadas? Claramente no.

Este es un problema que ya ha sido abordado por otras legislaciones que han establecido la obligación del responsable de la base de datos de informar a los titulares de que su información ha sido expuesta a personas no autorizadas, y en algunos casos eventualmente expuesta. Primero se consagró en Estados Unidos –en el Estado de California en el año 2003- y actualmente la mayoría de los Estados cuentan con la obligación de notificar en caso de que suceda una brecha de datos. Europa igualmente cuenta con una obligación general para sus estados miembros establecida en el RGPD que, ante casos de incumplimiento, establece multas de hasta el 4% del volumen de ingreso anual de la empresa o 20 millones de euros (el que sea mayor).

La normativa de Estados Unidos destaca por tener una concepción de consumidor del titular de los datos personales, generándose usualmente una relación de consumidor-empresa al momento de la notificación, considerando la inclusión de organismos públicos frente a brechas de datos más graves. En cambio el modelo europeo prefiere una comunicación que suele darse primero con la autoridad de protección de datos personales, y solo en caso de ciertas categorías de datos o cuando las filtraciones son de mayor gravedad se da una comunicación directa con el ciudadano.

Muchos países, entre ellos Chile, en el proyecto de reforma que "Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales", han comenzado a dar un paso adelante en instaurar esta obligación.

Lo primero que ha de analizarse en estos casos es qué se ha de entender por brecha de datos, para poder luego exigir la notificación de esta a las personas cuya información ha sido expuesta. Estas definiciones son variadas, no encontrándose una definición absoluta de qué podemos entender por brecha de datos.

El Ponemon Institute, organismo que mantiene un informe periódico en que se examinan las tendencias en brechas de datos, las define como "*un evento en que el nombre de un individuo y un registro médico o financiero o tarjeta de crédito es potencialmente puesto en riesgo, sea en formato electrónico o papel*". Otra definición nos señala que es "*un incidente en que información sensible, protegida o confidencial ha sido potencialmente vista, robada o usada por un individuo no autorizada para hacerlo*" [1].

En este sentido ambas definiciones aportan criterios claros de que ha de considerarse como brecha de datos. En primer lugar, la cuestión relevante es la pérdida o puesta en riesgo de los datos personales. En segundo lugar, estos datos pueden ser de variada naturaleza, sea financiera, de salud o simplemente información personal que no caiga en las categorías anteriores. En tercer lugar, los medios por los cuales puede producirse una brecha de datos son tanto electrónicos, como por medio de papel.

Existe una determinada cantidad de brechas de datos que logramos conocer de la totalidad que se producen. Hemos de distinguir si han sido detectadas o no; si no es detectada, no recae sobre el responsable la obligación de reportar, no significando que no se posean otras obligaciones de seguridad con sus sistemas.

Luego de aquellas que son detectadas existen algunas que, por su insignificancia técnica o irrelevancia jurídica, no han de ser reportadas. Pero también hay algunas que debiendo ser reportadas no lo son, por ejemplo la brecha sufrida por Uber el año 2016 que recién fue revelada por la empresa a comienzos de este año. A continuación, están aquellas que son reportadas, sea a la autoridad fiscalizadora o a la persona afectada, dependiendo de la manera en que se configure la obligación legal.

Así la notificación de una brecha pasa por distintos momentos, pudiendo mediar un espacio de tiempo desde que esta se produce hasta que es detectada y notificada. Por ejemplo, en la brecha de EQUIFAX del año pasado al no haber realizado las actualizaciones correspondientes a los servidores esto permitió la realización de un ataque que no fue detectado por varios meses, en que finalmente una auditoría de la empresa revelo la envergadura del ataque. La obligación de reportar la brecha de datos sólo opera en los supuestos de que las brechas es conocida, quedando fuera de la obligación de reporte aquellas que no son conocidas por el responsable de la base de datos. Finalmente si se aplica o no una sanción, es algo que se suele determinar en atención a la gravedad

de la brecha y el descuido de los responsables de las bases de datos.
En Chile actualmente no está vigente una obligación de reporte de brechas de datos, y la información que es puesta en conocimiento de las personas por parte de las empresas no nace de una obligación originada en nuestra legislación de datos personales como en otras jurisdicciones. Así nos encontramos dentro del grupo de países que cuenta con un sistema de notificaciones puramente voluntario y auto regulatorio. En este modelo es el propio organismo, cuya base de datos se ve vulnerada, el que decide notificar de que su base de datos ha sido vulnerada [2]. Se pondrá la información en conocimiento de las personas en atención a obligaciones contractuales contraídas con ellas o en atención a la normativa de protección del consumidor, pero no como una obligación específica de protección de datos y que satisfaga criterios en atención a la protección de la información. Esto es propio de legislaciones desactualizadas.
Otro modelo -y este es el propuesto en la reforma- es aquel en que definiéndose con claridad la existencia de un obligación de reportar, está sujeta a excepciones en el caso de que se cumplan ciertos requisitos que señala la propia normativa. Podríamos subdividir este modelo en uno de excepciones amplias y otro de excepciones más restringidas [3]. Este modelo es el seguido por la mayoría de las legislaciones que consagran esta obligación.
En tercer lugar existe un modelo más rígido en que la normativa no sólo indica los casos en que ha de notificarse ante una brecha de datos, sino que las normas indican cual ha de ser la estructuración del sistema de seguridad informática dentro de la empresa u organización que reporta los incidentes de seguridad. Este modelo solo lo hemos detectado en regulaciones especializadas de mercados altamente amenazados por ataques informáticos, como en la legislación en materia de ciberseguridad financiera de Nueva York.
En definitiva la obligación de notificación en caso de brecha de datos personales es bastante simple, es la puesta en conocimiento que se realiza al titular de los datos personales de que su información ha sido robada, vulnerada o se encuentra amenazada. Son las circunstancias que rodean a esta, la complejidad de los sistemas informáticos, vulnerabilidades humanas o la naturaleza discreta de los ataques que pueden pasar inadvertidos por largos períodos de tiempo, que hacen a veces difícil su cumplimiento. Así esta podrá variar en tiempo y forma que se realice en atención a la manera en que se consagre.
En el proyecto de reforma de la ley de datos personales se consagra un deber general de seguridad, detallándose como una obligación de implementar medidas de seguridad en los sistemas de información. Entre los deberes del responsable de la base de datos -en el artículo 14 quinquies- se consagra la obligación de reporte, estableciendo lo siguiente:

"Artículo 14 quinquies.- Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos deberá reportar a la Agencia de Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio o afectación para los titulares.

El responsable de datos deberá registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas.

La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional."

En este sentido la nueva legislación adopta el modelo en que definiendo lo que ha de entenderse por brecha de datos da lugar a dos notificaciones. Primero una general, que ha de reportarse a la Agencia de Protección de Datos Personales las vulneraciones "*que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate, o la comunicación o acceso no autorizados a dichos dato cuando exista un riesgo razonable que con ocasión de estos incidentes se genere un perjuicio o afectación para los titulares*".
En tanto consagra una segunda obligación que exige un estándar algo más elevado en que junto con cumplir las condiciones anteriores que motivan el reporte a la Agencia de Protección de Datos, cuando las vulneraciones a las medidas de seguridad involucren "*datos personales sensibles o a datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable deberá también efectuar esta comunicación a los titulares de estos datos*".
Lo anterior revela que la propuesta de reforma se aproxima al modelo europeo, primando la obligación de reportar en primer lugar con el organismo responsable de la protección de datos, dejando la comunicación directa con los titulares cuando esta involucra cierta clase de datos, que la ley se encarga de definir.
En el caso de las filtraciones de tarjetas de crédito -de haber estado vigente esta norma- probablemente los titulares no se habrían enterado por redes sociales, sino que su banco se habría contactado directamente con ellos por medio de un mensaje; o si la filtración fuese de gran envergadura, probablemente habría realizado una publicación oficial por algún medio de prensa cumpliendo las exigencias de la norma. Esta nos señala que la "*comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional*".
E inclusive encontrándose vigente esta norma las exigencias de ella son vagas, pide que sea "*lenguaje claro y sencillo*", indicando "*las posibles consecuencias de las vulneraciones de seguridad*" y señalando "*las medidas de solución o resguardo adoptadas*". Se hace necesario precisar -a través del Reglamento de la ley o mediante la dictación de directrices por el organismo encargado de protección de datos- dotar de contenido estas exigencias que, por sí solas, resultan insuficientes para dar garantías a los consumidores que frente a estos se encuentran en una situación de gran indefensión. Es difícil imaginar a las instituciones afectadas permitiendo el ingreso a sus clientes para monitorear y determinar cuáles datos fueron filtrados o si la naturaleza de la falla permite una nueva filtración.
Estos casos revelan la urgente necesidad de contar en nuestro país con una ley de protección de datos personales que esté a la altura de las exigencias y riesgos que enfrenta nuestro país. Una ley que proteja a los ciudadanos, que otorgue las facultades al organismo encargado de proteger los datos que permita una efectiva fiscalización y establezca obligaciones clara a los responsables de bases de datos de manera que sean capaces de cumplir las exigencias de la nueva normativa. De no ser así, lamentablemente estos ataques seguirán sucediendo y seremos nosotros quienes no podrán defenderse en el entorno digital. (Santiago, 30 julio 2018)

[1] Solove, D., & Schwartz, P. (2011). *Privacy Law Fundamentals.* IAAP.

[2] Tropina, T., & Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and*

National Security. (S. Briefs, Ed). Springer.

[3] Fowler, K. (2016). *Data breach preparation and response?: breaches are certain, impact is not*. Elsevier.

Esta columna está basada en el trabajo presentado en el V Simpósio Internacional LAVITS: "Vigilância, Democracia e Privacidade na América Latina: vulnerabilidades e resistências", realizado entre el 29 y 30 de noviembre del 2017 en la Universidad de Chile.