lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

MERCADOS DE DATOS E INCIDENTES DE SEGURIDAD

Mercados de dados e incidentes de segurança

Data markets and security incidents

José Pablo Lapostol Piderit[a]

[(a)] Alumno de 5to año de Derecho Universidad de Chile. Ayudante de Filosofía Moral (UCH) y del Centro de Estudios en Derecho Informático (UCH). E-mail: jp.lapostol@gmail.com.

Resumen

En este trabajo nos proponemos examinar el mercado de datos y en especial, la configuración legal de la obligación de notificación en caso de brecha de datos personales. No existe normativa vigente en Chile que obligue al responsable de una base de datos el reportar a las personas cuando sus datos sean comprometidos por un ataque informático. Esto pone a los titulares de datos personales en una situación desventajosa al no poder tomar medidas para prevenir posibles perjuicios que acarree la exposición no deseada de sus datos. El trabajo busca examinar el mercado de datos existente, tanto legal e ilegal y la manera en que han venido ocurriendo incidentes de seguridad durante los últimos años. Se analizan los modelos de legislación más paradigmáticos en la materia como referencia para la reforma de esta materia en Chile. Finalmente se analiza la propuesta de reforma a la ley de datos personales de Chile y se proponen una serie de reflexiones y propuestas sobre la materia.
Palabras clave: Mercados de datos; Brecha de datos; Notificación; Datos personales.

Resumo

Neste artigo, propomos examinar o mercado de dados e, em particular, a configuração legal da obrigação de notificação em caso de violação de dados pessoais. Não existe uma regulamentação atual no Chile que exija que a pessoa responsável por um banco de dados informe às pessoas quando seus dados são comprometidos por um ataque de computador. Isso coloca os detentores de dados pessoais em situação de desvantagem ao não poder tomar medidas para prevenir possíveis danos causados pela exposição indesejada de seus dados. O trabalho procura examinar o mercado de dados existente, tanto legal quanto ilegal e a forma como os incidentes de segurança ocorreram nos últimos anos. Os modelos mais paradigmáticos de legislação no

assunto são analisados como referência para a reforma deste assunto no Chile. Finalmente, a proposta de reforma da lei de dados pessoais do Chile é analisada e uma série de reflexões e propostas sobre o assunto são propostas.
Palavras-chave: *Mercado de dados; Violação de dados; Notificação; Dados pessoais.*

Abstract

In this paper we propose to examine the data market and in particular, the legal configuration of the data breach notification in case of breach of personal data. There is no current regulation in Chile that requires the responsible of a database to report to people when their data is compromised by a computer attack. This puts holders of personal data in a disadvantaged situation by not being able to take measures to prevent possible harm caused by the unwanted exposure of their data. This paper seeks to examine the existing data market, both legal and illegal and the way in which security incidents have been occurring over the past few years. The most paradigmatic models of legislation in the matter are analyzed as a reference for the reform of this matter in Chile. Finally, the proposal to reform the personal data law of Chile is analyzed and a series of reflections and proposals on the subject are proposed.
Keywords: *Data markets; Data breachs; Notification; Personal data.*

INTRODUCCIÓN

En la actualidad es difícil imaginar alguna actividad que no requiera datos. Desde que ingresamos a la sociedad pasamos a tener datos, se nos identifica, se nos otorga un nombre, edad, género, elementos que confluyen y que nos identifican como personas. La filosofía nos habla de "*infoesfera*" (Floridi, 2013) como el nuevo campo de convivencia humana, un espacio en que la información es el factor determinante de operación y responsabilidad moral.

Toda esta modernización ha sido posible gracias a los avances tecnológicos, la facilidad de replicar la información, de transmitirlas, de almacenarla, de comprenderla. La información es el elemento clave de la economía, y considerándola de una manera atomista esta se encuentra conformada por el dato, una unidad que contiene información (Johns, 2016).

En esta evolución de la información quizás uno de los cambios mas grandes en la manera de conocerla es el Big Data (Kalyvas & Overly, 2014). Inmensas cantidades de información que coordinada permite vislumbrar caracteres y perfiles de la sociedad humana que en la antigüedad jamás podríamos haber conocido. Nuestros datos procesados a través de algoritmos complejos y avanzados permiten desnudar parte de nuestra intimidad e identidad (Citron & Pasquale, 2014).

La gran acumulación de datos por parte de gobiernos, empresas y otras instituciones ha llevado a que estas sean objetos de ataques por parte de criminales quienes en busca de variados fines atacan base de datos en busca de la información que estas contienen (Lu & Shen, 2015).

Frente a estos ataques se ha erigido una obligación, una obligación simple pero extremadamente relevante. La puesta en conocimiento al ciudadano de que su información ha sido comprometida por un ataque o descuido informático (Fowler, 2016). Podría parecer lo más evidente que si la información es precisamente de uno, no el sentido de propiedad siquiera, sino como una cualidad esencial que nos define y caracteriza seamos los primeros en ser informados de que hemos sido comprometidos y de que estamos expuestos.

En este trabajo nos proponemos examinar en primer lugar los actores del mercado de datos y la configuración de un mercado legal e ilegal de estos. En segundo lugar nos detendremos en la definición de una brecha de datos y cuáles son los modelos de cumplimiento de la normativa de notificación, para posteriormente analizar el panorama de brechas de datos en diferentes mercados. Posteriormente examinaremos la normativa que rige en Estados Unidos[1] y en la Unión Europea[2] en materia de notificación de brecha de datos personales. Finalizando examinaremos la reforma a la normativa chilena de protección de datos personales, en especial la manera en que se consagro en el proyecto de reforma de la ley 19.628 la obligación de notificar una brecha de datos personales[3]. Por último ofreceremos una serie de reflexiones sobre la obligación de notificación y propuestas a considerar para posibles reformas o reconsideraciones sobre esta obligación.

ACTORES EN EL MERCADO

Existe un mercado para los datos de las personas, quienes los demandan y quienes los ofrecen, y el bien es nuestra información, nuestros datos.

Como todo mercado este tiene actores, quienes compran y venden los bienes que se transan en este. La diferencia más relevante, y que otorga mayor claridad al momento de examinar las obligaciones sobre nuestros datos es entre quienes entregan información (personas) y aquellos que la captan

[1] En adelante USA.
[2] En adelante UE.
[3] En adelante NBDP.

(pudiendo ser tanto instituciones privadas como públicas).

El primero de los sujetos de este mercado son las personas, estas se encuentran inmersas en una sociedad en que conviven e interactúa con otros. Esta convivencia implica una cierta publicidad, una necesaria puesta disposición de nuestra información con el resto de las personas con las que nos relacionamos. Las personas poseemos una cantidad inmensa de datos, que nos caracterizan, determinan y en definitiva conforman parte de la misma persona (Floridi, 2013).

Hasta tiempos recientes la información de los individuos de la sociedad no podía ser captada más allá de lo que ellos compartieran. Esto ha cambiado en la actualidad, con el avance de los mecanismos de comunicación, la inclusión de redes sociales y la evolución de tecnologías de vigilancia, nuestros datos pueden ser recopilados con mayor facilidad (Assange, 2013).

Un segundo actor del mercado son las empresas u organizaciones privadas que captan nuestros datos. Sean movidos por el modelo de negocios que implementan, la necesidad de poder competir en el mercado para lo cual requieren información de los consumidores, o sea para captar la información que las personas les proveen, el sector privado es un gran demandante y captador de información de las personas (Banks & Said, 2006).

Son muchos los elementos que han producido el cambio en la captación privada, pero quizás los elementos más relevantes son dos las redes sociales y el sistema financiero moderno. Las redes sociales representan quizás el cambio más paradigmático de nuestra relación con la distribución de nuestra información por redes privadas, pues esta entrega es absolutamente voluntaria sin mediar coerción (Taylor, Bakshy, & Aral, 2013). También las características de la economía moderna obligan a participar en el sistema financiero moderno. Nos llevan a relacionarnos con instituciones pertenecientes a ese mercado que también captan grandes cantidades de información de las personas (Nath, 2015).

Otro actor del mercado es el Estado, quien opera como un doble agente, regulando y demandando datos. El Estado como captador de procesa y sistematiza una gran cantidad de datos de parte de sus ciudadanos, desde su nacimiento hasta su fallecimiento el ciudadano le entrega información de manera voluntaria, pero también involuntaria (Bercea, Nemtoi, & Ungureanu, 2010). Este agente ha demostrado ser un gran captador de datos, sea por medio de la vigilancia, y también al proveer

servicios, a los más necesitados que no pueden acceder a ellos en el mercado privado.

Así este mercado se configura entre quienes regulan, quienes entregan datos y quienes los demandan. En la obtención de datos es donde existe un claro conflicto entre los diferentes actores, encargándose la ley de regular tanto su entrega, comercialización o captación. En tanto la obtención de los datos sea dentro del marco regulatorio, este mercado tendrá la cualidad de ser legal. Pero es posible cuando la demanda de los datos no puede ser suplida de manera lícita es posible hacerlo de manera ilícita. En este contexto donde suelen producirse robos de información.

Así otro actor que confluye al mercado de datos son los criminales, quienes mediante ataques a las bases de datos que contienen la información roban para luego vender los datos de las personas, o para cometer los delitos ellos mismos (Ablon, Libicki, & Golay, 2014).

Esta manera de hacerse de los datos ha venido de la mano con el cambio en la manera de realizar ataques informáticos (Bayuk, Healey, Rohmeyer, Sachs, Schmidt, & Weiss, 2012). Estos en un comienzo se caracterizaban por ser más "*públicos*" en su manera de realizarse, interrumpiendo servicios o exponiendo mensajes de que el ataque se estaba llevando a cabo. Pero luego estos han ido evolucionando, pasaron de ser notorios a ser sigilosos.

Buscando una extracción sistemática de la información disponible en la base de datos, rootkits, ingeniería social, troyanos, todas herramientas que permiten a un atacante infiltrase en un sistema y permanecer en él en espera de su oportunidad de extraer la información y salir (Egele, Scholte, Kirda, & Barbara, 2011).

Un ataque informático detenta una serie de pasos claramente distinguibles. Primero existe una infiltración, en que por diversos los atacantes ganan acceso a las bases de datos. Luego existe un despliegue dentro de la base de datos que fue penetrada por el atacante intentando abarcar la mayor cantidad posible de bases. Posterior a eso se produce la extracción de la información que interesa al atacante. Por último existe un retiro de la base de datos que fue atacada (Engebretson, 2011).

Es en este contexto en que las leyes encargadas de regular los datos personales de las personas comienzan a considerar entre las obligaciones de los responsables de las bases de datos, la notificación del ataque. Específicamente de la brecha de datos, sea ante el riesgo o la certeza de que se hayan podido obtener ilícitamente datos que las personas han entregado al responsable de la base de

datos.

Esta obligación de notificación es un medio de poner en conocimiento a la persona de que su información ha sido vulnerada. Ya que ellas se encuentran en una situación desventajosa al resultar extremadamente complejo entrar en conocimiento de la situación de que se ha producido un ataque informático y sus datos han sido comprometidos (Solove, 2013).

BRECHA DE DATOS

Las legislaciones para poder otorgar certeza a los diferentes participantes del mercado han de definir que se ha de entender por brecha de datos para poder luego exigir la notificación de esta a las personas cuya información ha sido vulnerada. Estas definiciones son variadas, no encontrándose una definición absoluta de que podemos entender por brecha de datos.

El Ponemon Institute define una brecha de datos 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" (Ponemon Institute, 2017, paginación indisponíble). Otra definición, tomada de la legislación de New Jersey es "un incidente en que información sensible, protegida o confidencial ha sido potencialmente vista, robada o usada por un individuo no autorizada para hacerlo" (Solove & Schwartz, 2011, paginación indisponible).

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. Hemos de distinguir si esta detectadas o no, si no es detectada no recae sobre el responsable ninguna clase de obligación legal. Luego de aquellas que son detectadas existen algunas que por su insignificancia o no relevancia jurídica no han de ser reportadas. Pero también hay algunas que debiendo ser reportadas no lo son. Luego están aquellas que son reportadas, sea a la autoridad fiscalizadora o a la persona, dependiendo de la manera en que se configure la obligación legal. Finalmente de aquellas reportadas, no todas son

sancionadas y/o no todas son demandadas por parte de los ciudadanos.

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 (Allodi & Massacci, 2013). La obligación de reportar la brecha de datos solo 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[4]. La sanción, o no, es algo que se determina en atención a la gravedad de la brecha y el descuido de los responsables de las bases de datos (Trautman & Ormerod, 2017).

Podríamos definir la obligación de notificación en caso de brecha de datos personales como 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.

El examen de la literatura nos ha llevado a detectar tres posibles formas de estructurar la obligación de notificación de brecha de datos.

En primer lugar un sistema puramente voluntario y auto regulatorio. En este modelo es el propio organismo cuya base de datos se ve vulnerada que decide notificar ante la realización de que su base de datos ha sido vulnerada (Tropina & Callanan, 2015). Este modelo es propio de legislaciones desactualizadas.

Otro en que definiéndose con claridad la existencia de un obligación de reportar esta sujeta a excepciones en el caso de que se cumplan ciertos requisitos que señala la propia. Podríamos subdividir este modelo en uno de excepciones amplias y otro de excepciones más restringidas(Fowler, 2016). Este modelo es el seguido por la mayoría de las legislaciones.

En tercer lugar un modelo más rígido en que la normativa no solo indica los casos en que ha de notificarse ante una brecha de datos, sino que las normas indican de igual 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 nueva legislación en materia

[4] Pueden existir casos en que un tercero reporte al responsable de la base de datos de que la información ha sido comprometida poniendo al responsable en conocimiento de la brecha y por consiguiente obligándolo a reportarla.

de ciberseguridad financiera de Nueva York.

La obligación de reportar en definitiva se configura en que el responsable de la base de datos ha de detectar las vulneraciones e informar a las personas, titulares de los datos, que su información se encuentra en riesgo, pudiendo transitar las legislaciones entre estos modelos.

PANORAMA DE BRECHAS DE DATOS

A pesar de consagrarse la obligación de NBDP, son numerosos los casos que no son reportados por parte de quienes recolectan datos, o que los notifican de manera tardía. Esto es constatado tanto en la literatura especializada como en notas de prensa, en que día a día se descubren nuevas brechas que han pasado inadvertidas (Apostle, 2017). De igual manera todos los captadores son atacados, existiendo diferencias en atención a la clase de datos que están almacenados en las bases de datos.

La literatura nos indica que este comportamiento de no reportar o de reportar tardíamente se deriva de la gran variedad de costos que ha de soportar el responsable de la base de datos al momento de notificar una brecha de datos. Estos costos podemos dividirlos en directos e indirectos (Romanosky, 2016).

Los costos directos que se soportan debido a una notificación de brecha de datos los encontramos más relacionados a aquellos que fueron provocados de una manera clara y evidente por la brecha de datos que se produjo o que podría producirse. Entre estos podemos encontrar a la creación de una lista de contactos post-brecha, la notificación realizada, la contratación de equipos forenses para detectar y evaluar la brecha, los gastos de compliance, etc. (Mossburg, Fancher, & Gelinne, 2016).

Existen también los costos indirectos que son aquellos que sufre la institución captadora de datos de una manera más distante, no relacionada de una manera inmediata con la brecha de datos. Entre ellos están la pérdida de confianza en la institución, la pérdida de valor de la marca o empresa, o la pérdida de competitividad (Rosati, Cummins, Deeney, Gogolin, Werff, & Lynn, 2017).

Estos costos, directos e indirectos, son asumidos por los captadores de datos. Pero estos costos varían en atención a las normas de los países por ejemplo existe un clara diferencia, en tanto mas rigurosa las normas mayor será el corto de reporte, pudiendo en consecuencia encontrar comportamiento

oportunista y de adversidad hacia la norma. El Ponemon Institute señala que los países en vías de desarrollo no imponen tantos costos a las organizaciones, en tanto en países más desarrollados resultan más costosos(Ponemon Institute, 2017). También hay un grupo de países que mediante altas multas resultan en un costo alto de prevención y reparación (Greenleaf & Hui-ling, 2012; Greenleaf & Park, 2012).

También los costos suelen ser más altos en mercados más regulados, como en salud, finanzas o educación. Estos mercados suelen exceder en costos a mercados menos regulados como el sector público, transporte o medios de comunicación (Ponemon Institute, 2017).

Existen grupos de captadores de datos que suelen ser más atacados, por ejemplo destaca la industria financiera, servicios, industrias y el área de salud. Este grupo de organizacionesson aquellas que sufren n mayor número de ataques informáticos (Ponemon Institute, 2017).

La explicación de lo anterior lo encontramos en varios factores. En primer lugar, el mercado de datos se centra especialmente en datos financieros de las personas, datos sensibles y espionaje empresarial (Booysen & Neo, 2017). Así estos grupos de organizaciones son las que recopilan esta clase de datos con mayor sistematicidad, a diferencia de los sectores por ejemplo energético, de investigación o de transporte (Holt, Smirnova, & Chua, 2016).

Otra cuestión relevante es que parte de los datos a veces no llegan siquiera al mercado negro para ser comercializados, siendo una parte importante de los ataques informáticos destinados a espionaje entre países o empresas (Gragido, Molina, Pirc, & Selby, 2012). También las bases de datos que contienen datos de la salud de las personas suelen ser comercializadas a un precio mucho mayor que, por ejemplo, las bases de datos financieras (Samani, 2016).

Junto con lo anterior las empresas se ven fuertemente afectadas por las brechas de datos, pues al verse obligadas a notificar la vulneración de la seguridad de sus sistemas los consumidores pierden la confianza en ellos, produciéndose incluso la pérdida de clientes y el fin de contratos que se relacionan con las áreas que han sido atacada[5] (Jenkins, Anandarajan, & D'Ovidio, 2014).

Otro costo relevante y que es propio de los riesgos cibernéticos son los ciberseguros. Estos seguros

[5] La paradoja se da en que cuando una organización es atacada es menos probable que sufre un segundo ataque.

especializados en riesgos informáticos tienen cualidades interesantes, junto con permitir soportar ciertos costos a las organizaciones afectadas por una brecha de datos, son quizás el regulador privado más importante de medidas de seguridad. Pues obligan a la organización que los contrata a adecuarse a los estándares que esta impone para poder reembolsar gastos (Gordon, Loeb, Lucyshyn, & Zhou, 2015).

Usualmente los ciberseguros se valen de estándares aceptados en el mercado de ciberseguridad para proveer sus servicios, promoviendo la uniformidad.

Creemos que la atención a la manera en que se comercializan nuestros datos por mercados legales e ilegales y los costos a los que se ven expuesto las organizaciones que captan nuestros datos han de servir para guiar las reformas o implementaciones de la NBDP.

IMPLEMENTACIÓN DE NBDP EN USA Y UE

Para un examen de la implementación de la NBDP nos centraremos en dos legislaciones que estimamos son las más paradigmáticas, y que han servido de modelo para este tipo de leyes. Estas son el sistema de NBDP de USA y por otro lado el de la UE.

Recientemente la normativa de notificación en caso de brecha de datos, en USA y UE, destacaba por una cualidad que es la sectorialidad (Solove & Schwartz, 2011; Loenen, Kulk, & Ploeger, 2016). Esto es, normas particulares que no consagraban una obligación general y clara en caso de una brecha de datos, debiendo recurrir a cuerpos especiales de normas para poder determinar si corresponde o no realizar una notificación al titular de los datos o la autoridad responsable.

Otra cualidad que se destaca de estos sistemas es su constante evolución en su litigación (Romanosky, Hoffman, 2012). En USA ha resultado complejo otorgar indemnizaciones por el daño sufrido a las personas por brecha de datos, muchas veces denegando el acceso a las cortes. Similar situación ocurre actualmente en la UE.

El modelo estadounidense es un modelo que radica más en la notificación directa a la persona de que sus datos han sido vulnerados, en cambio el modelo europeo se caracteriza por una notificación a la autoridad encargada de la protección de los datos de los ciudadanos. Este era el criterio de distinción

más claro en la manera en que esta obligación se configuraba (Laube & Böhme, 2016). Pero a partir de la puesta en vigencia de la nueva normativa de Protección de datos personales, que entrara en vigor en mayo del 2018, el modelo europeo ha avanzado en una normativa mucho más estricta y clara en materia de protección de datos personales.

USA fue el primer que conto con una normativa de obligación de NBDP, siendo esta instaurada el año 2002 en el Estado de California. Actualmente 47 estados consagran la obligación de reporte de brecha de datos, y las definiciones de esta son variadas (Markou, 2015).

En el modelo estadounidense la configuración de la obligación de notificar en caso de una brecha de datos se ha dejado a regulación estatal resultando ilustrativo como distintas definiciones conllevan una mayor o menor carga de las empresas al momento de reportar incidentes. Algunas oscilan en que basta la constatación de un acceso no autorizado para obligar la responsable a notificar. En cambio otras legislaciones se enfocan en la constatación de un riesgo cierto a los datos de las personas para que proceda la notificación (Wehbé, 2017).

A modo de ejemplo la regulación de New Jersey propone una definición amplia de brecha de seguridad, y exige un reporte a la Policía y a la Fiscalía, a través de la policía estatal, de cualquier brecha de seguridad en registros informáticos que haya sido, o se crea razonablemente que haya sido haya sido accedido por parte de una persona no autorizada. Sin embargo New Jersey no siempre requiere en el reporte del incidente al cliente cuando no existe posibilidad de mal uso de la información que pudo haber sido sustraída. Las mejores prácticas requieren que el "*Chief of Information Security*" (CISO) o una empresa externa TIC experta avalen esta conclusión (Setptoe & Johnson, 2016).

Pero también es posible que existan casos, en que no siendo obligatorio el reporte del incidente informático en atención a las leyes estatales, este sea recomendable o sea exigible el reporte de este al titular de los datos. Por ejemplo, cuando existen otros cuerpos normativos que exijan el reporte al cliente de las gestiones que se llevan a cabo con su información o el posible daño a la reputación de una empresa al existir un reporte no controlado de la brecha de seguridad. En estos casos el reporte voluntario da al responsable de la base de datos la posibilidad de controlar la información de tales incidentes, a diferencia de si esta información se filtra por medios no controlados por el responsable (Fowler, 2016).

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 (Solove & Schwartz, 2011).

La UE mantenía hasta hace poco una legislación similar a la estadounidense en materia de notificación de brecha de datos. Por ejemplo era necesario recurrir a las normas que regulaban la protección de datos personales de cada Estado Miembro para encontrar la obligación de notificación, y solo existía la obligación de notificación en ciertos cuerpos de normas especiales de la Unión (Markou, 2015). Pero a partir de la entrada en vigencia de la nueva normativa de protección de datos este criterio ha cambiado, creando una obligación general de reporte para los Estados Miembros de la Unión. Así a diferencia del modelo estadounidense que aún no adopta una obligación federal de notificación de brecha de datos, en la actualidad la UE se encuentra transitando entre dos modelos, de una configuración dispersa a una configuración unificada estableciendo los requisitos mínimos que ha de cumplir la notificación en caso NBDP de los Estados Miembros (Schünemann & Baumann, 2017).

La nueva obligación impone al responsable de la base de datos la notificación a la autoridad supervisora sin tardanza injustificada, y dentro del plazo de 72 cuando hay certeza de la existencia de una brecha. Sin embargo permite cuando sea poco probable que la brecha de datos represente algún riesgo para los derechos y libertades de las personas naturales no se exigirá el cumplimiento de este plazo.

El responsable de la base de datos ha de notificar a los titulares de los datos sin tardanza injustificada frente a las vulneraciones que representen un alto riesgo.

Quizás el cambio más radical lo representan las sanciones al no cumplimiento de la obligación. Las autoridades encargadas de la protección de datos personales pueden aplicar multas de 20 millones de euros o el 4% de las ganancias anuales del año financiero que precedió a la brecha, cualquiera sea la más alta. También le da a los ciudadanos de los Estados Miembros la posibilidad de reclamar para reclamar compensación o intentar acciones colectivas (Gutwirth, 2016).

Como es posible muchas de las deficiencias que se han hecho notar de la regulación estadounidense han sido resueltas por parte de la GDPR. Especialmente al consagrar multas que incentivan a un

manejo responsable de los datos por parte de los responsables de bases de datos y al otorgar mayor certeza al momento de entablar acciones judiciales.

De lo anterior vemos claramente cómo se configuran dos modelos, uno que se ha mantenido en normas especiales, que no sanciona de una manera dura a los responsables de datos y que dificulta el acceso de los sujetos al reclamo ante los tribunales. Y otro que reconociendo la relevancia de los datos personales otorga una mayor protección a los ciudadanos, estableciendo sanciones altas ante brechas de datos y permitiendo acceder a los tribunales con mayor facilidad.

PROTECCIÓN DE DATOS Y BRECHA DE DATOS EN CHILE

El panorama de la protección de datos personales es diverso. Nos encontramos con una consagración de un derecho a la privacidad en nuestra Constitución, sin un recurso constitucional especializado en la protección de datos personales, pero contando el derecho a la privacidad tutela en la acción de protección general que otorga la Constitución (Violler, 2017).

Contamos normativa especial de protección de datos personales, la Ley n. 19.628, siendo reconocida por ser la primera de Sudamérica, pero de igual manera sufre debido a su desactualización.

La acción que se consagra de protección de datos personales destaca por su lentitud e ineficiencia para otorgar una eficaz protección en casos de protección de datos personales, debiendo recurrir a otras vías para una adecuada protección de los datos personales (Anguita Ramírez, 2007). No existe en esta norma una obligación de notificación de vulneración, encontrándose esta norma en el modelo de reporte voluntario de la brecha de datos personales.

Muchos han señalado la deficiente defensa de los datos personales de la actual normativa que rige en Chile y han reclamado por su actualización. En este contexto se propone la modernización de la legislación de protección de datos personales (Gobierno de Chile, 2015).

En noviembre de 2015 el gobierno de Chile hizo pública la agenda digital 2020. El objetivo de esta agenda es cumplir con compromisos asumidos al ingresar a la OCDE y mejorar las regulaciones de materias tecnológicas, considerando dentro de las medidas de la agenda la modernización de la regulación de datos personales (Derechos Digitales, 2017). Se ingresó un proyecto de ley que se

encuentra actualmente en tramitación que ha de modificar la ley 19.628, este proyecto pretende modernizar la protección de datos personales en Chile, considerando entre varias modificaciones una obligación de reporte de brecha de datos personales[6].

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. Entre los deberes del responsable de la base de datos en el Art. 14 quinquies, se consagra la obligación de reporte, este artículo indica:

> *Artículo 14 quinquies.* - ***Deber de reportar las vulneraciones a las medidas de seguridad. El responsable de datos debe 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 dichas vulneraciones se refieran a 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****. Esta comunicación debe 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 debe 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 conlleven "***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***". 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***".

[6] Boletín N° 11144-07.

De la distinción clásica de modelos de notificación en caso de brecha de datos personales el modelo chileno se encuentra más relacionado con el europeo, exigiendo un reporte de una gran cantidad de vulneraciones a la Autoridad. Así el artículo solo impone la obligación de notificar en caso de brecha de datos personales en que las brechas involucren ciertos datos. El artículo también se encarga de indicar brevemente las condiciones mínimas que ha de cumplir la notificación, cuestión que ha preocupado a las autoridades, al requerir que esta sea comprensible para las personas.

Como podemos ver Chile está intentado avanzar en la defensa de los datos de sus ciudadanos, comprometiéndose a mejorar las condiciones de protección de los datos personales de las personas. Pero queda aún pendiente que este proyecto de ley finalice su tramitación y sea finalmente convertido en ley de la República.

CONCLUSIONES

Como podemos ver se cumple lo indicado por expertos latinoamericanos que de donde más se nutre la normativa de protección de datos personales de Latinoamérica es del modelo europeo, pero lamentablemente en este caso es de la normativa europea más antigua que moderna. Teniendo la normativa un "esqueleto europeo" pero no acercándose a la rigurosidad de esta que vincula protección de datos como una cuestión fundamental de su ciudadanía.

Por tanto quedamos nuevamente con un paso atrás en parte emulando ciertos defectos de la normativa estadounidense, al no encontrarse un fácil acceso a los tribunales por parte de los ciudadanos al reclamar de las vulneraciones de sus datos personales.

Estimamos que es necesario una elevación a categoría constitucional de la protección de datos personales, sea consagrando como un derecho fundamental la autodeterminación informativa y/o consagrando un derecho al "*habeas data*" en nuestra normativa constitucional.

Otra cuestión relevante que estimamos ha de considerarse, es la especial protección de datos sensibles, pudiendo considerar una normativa y sanciones especiales cuando los datos que sean vulnerados sean datos sensibles de las personas. Estos son los más buscados y son aquellos que son objeto de una mayor cantidad de ataques, por lo que la normativa de los países ha de tenerlo en consideración.

También uno de los defectos que hemos notados en la literatura es que esta se centra especialmente en la brecha de datos que sufren los captadores privados, muchas veces resultando difícil encontrar antecedentes de estudio sobre brechas de datos producidos en órganos gubernamentales. Como señalamos al describir el mercado de datos, el Estado en sus variadas ramas y servicios es uno de los más grandes recopiladores de datos personales, por lo que creemos que un examen más comprehensivo necesario para determinar de manera adecuada el alcances de las brechas de datos.

A pesar de que queda camino por avanzar vemos con buenos ojos que por fin en Chile se esté avanzando en proteger de mejor manera los datos las personas, a pesar de las faltas que hemos señalado el proyecto de reforma de ley es sin duda un avance, en especial al considerar la información a las personas de que sus datos han sido captados por una persona no autorizada.

Los riesgos e incertidumbres de la revolución tecnológica dejan muchas veces al descubierto a los ciudadanos, quienes no pudiendo enfrentarse a los avances rápidos y complejos de la tecnología quedan desprotegidos en sus derechos. Estos derechos son lo que han de guiar las reformas e implementaciones de la regulación tecnológica en nuestro país, poniendo como centro siempre a las personas.

REFERENCIAS

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for Cybercrime Tools and Stolen Data. *National Security Research Division*.

Allodi, L., & Massacci, F. (2013). My Software has a Vulnerability, should {I} worry? *CoRR, abs/1301.1*. Recuperado el 30 de octubre de 2017 de http://arxiv.org/abs/1301.1275.

Anguita Ramírez, P. (2007). *La protección de datos personales y el derecho a la vida privada:* régimen jurídico, jurisprudencia y derecho comparado : análisis de la ley no. 19.628 sobre protección de la vida privada. Editorial Jurídica de Chile. Santiago de Chile.

Apostle, J. (2017). The Uber data breach has implications for us all. Financial Times [versión electrónica]. Recuperado el 30 de octubre de 2017 de https://www.ft.com/content/e2bf6caa-d2cb-11e7-a303-9060cb1e5f44.

Assange, J. (2013). Criptopunks. *La libertad y el futuro de internet, 240*. Recuperado el 30 de octubre de 2017 de http://catedras.ciespal.org/tecnopolitica/wp-content/uploads/sites/12/2016/02/Cypherpunks_Julian_Assange.pdf.

Banks, D. L., & Said, Y. H. (2006). Data Mining in Electronic Commerce. *Statistical Science, 21*(2), 234–246.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. Nueva Iorque: Wiley.

Bercea, L., Nemtoi, G., & Ungureanu, C. (2010). The government of state's power bodies by means of the Internet. *Journal of Computing, 2*(2), 25–27. Recuperado el 30 de octubre de 2017 de http://arxiv.org/abs/1002.3992.

Booysen, S., & Neo, D. S. S. (2017). *Can banks still keep a secret?* Bank secrecy in financial centres around the world. Cambridge: Cambridge University Press.

Citron, D. K., & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, *89*, 101–133.

Derechos Digitales. (2017). *La participación en la elaboración de la Política Nacional de Ciberseguridad:* Hacia un nuevo marco normativo en Chile. Recuperado el 30 de octubre de 2017 de https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf.

Egele, M., Scholte, T., Kirda, E., & Barbara, S. (2011). A survey on automated dynamic malware analysis techniques and tools. *ACM Computing Surveys*, *5*(2), 1–49.

Engebretson, P. (2011). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. *Vasa*, *178*.

Floridi, L. (2013). The ethics of information. In *Information*. Oxford: Oxford University Press.

Fowler, K. (2016). *Data breach preparation and response:* breaches are certain, impact is not. Nueva Iorque: Elsevier.

Gobierno de Chile (2015). Agenda Digital, Gobierno de Chile. *November*. Recuperado el 30 de octubre de 2017 de http://www.agendadigital.gob.cl/#/.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 13.

Gragido, W., Molina, D., Pirc, J., & Selby, N. (2012). *Blackhatonomics:* An Inside Look at the Economics of Cybercrime. Nueva Iorque: Elsevier.

Greenleaf, G., & Hui-ling, C. (2012, junio). Data privacy enforcement in Taiwan, Macau, and China. *Privacy Laws & Business International Report, 117, 11-13.*

Greenleaf, G., & Park, W. (2012). Korea's new Act: Asia's toughest data privacy law. *Privacy Laws & Business International Report*, *117*(117), 1–6.

Gutwirth, S. (Ed.) (2016). *Data Protection on the Move* [Vol. 24]. Berlín: Springer.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data Thieves in Action:* Examining the International Market for Stolen Personal Information. Nueva Iorque: Palgrave.

Jenkins, A., Anandarajan, M., & D'Ovidio, R. (2014). "All that Glitters is not Gold": The Role of Impression Management in Data Breach Notification. *Western Journal of Communication*, *78*(3), 337–357.

Johns, F. (2016, julio). Data Mining as Global Governance. In R. Brownsword, E. Scotford, & K. Yeung (Ed.). *The Oxford Handbook of Law*, Regulation and Technology. Oxford: Oxford University Press.

Kalyvas, J. R., & Overly, M. R. (2014). *Big Data: A Business and Legal Guide*. San Francisco, Taylor & Francis.

Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29–41.

Lu, Z., & Shen, H. (2015). *An Accuracy-Assured Privacy-Preserving Recommender System for Internet Commerce*. Recuperado el 30 de octubre de 2017 de http://arxiv.org/abs/1505.07897.

Markou, C. (2015, deciembre 15). The "Right to Be Forgotten": Ten Reasons Why It Should Be Forgotten. *Law Explorer*. Recuperado el 30 de octubre de 2017 de https://lawexplores.com/the-right-to-be-forgotten-ten-reasons-why-it-should-be-forgotten.

Mossburg, B. E., Fancher, J. D., & Gelinne, J. (2016). The hidden costs of an IP breach the hidden costs of an IP breach Cyber theft and the loss of intellectual property. *Deloitte Review*, (19), 106–121.

Ponemon Institute (2017). *Ponemon Institute's 2017 Cost of Data Breach Study:* Global Overview. Recuperado el 28 de noviembre de 2017 de https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), paginación indisponíble.

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Werff, L. van der, & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*, 146–154.

Samani, R. (2016). Warning: Healthcare Data Under Attack. *Dark Reading*. Recuperado el 28 de noviembre de 2017 de https://www.darkreading.com/partner-perspectives/intel/warning-healthcare-data-under-attack/a/d-id/1327287?piddl_msgorder=asc.

Romanosky, S., Hoffman, D., & Acquisti, A. (2012, enero). Empirical Analysis of Data Breach Litigation. *Workshop on Economics of Information Security*, *11*(1), 1–30.

Schünemann, W. J., & Baumann, M. O. (2017). Privacy, data protection and cybersecurity in Europe. In W. J. Schünemann & M. O. Baumann (Org.). *Privacy, Data Protection and Cybersecurity in Europe*. Berlín: Springer.

Setptoe & Johnson, L. (2016). Comparison of US State and Federal Security Breach Notification Laws. *Steptoe*. Recuperado el 28 de noviembre de 2017 de https://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf.

Solove, D. J. (2013). Autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho Y Tecnología*, *2*(2), 11–48.

Solove, D., & Schwartz, P. (2011). Privacy Law Fundamentals. *GW Law Faculty Publications & Other Works.* Recuperado el 28 de noviembre de 2017 http://scholarship.law.gwu.edu/faculty_publications.

Taylor, S., Bakshy, E., & Aral, S. (2013). Selection Effects in Online Sharing: Consequences for Peer Adoption. *Proceedings of the Fourteenth ACM Conference on Electronic Commerce.*, *1*(212), 821–836.

Trautman, L. J., & Ormerod, P. C. (2017). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. *American University Law Review*, *66*, 1–68.

Nath, T. (2015). How Big Data Has Changed Finance. *Investopedia.* Recuperado el 28 de noviembre de 2017 de https://www.investopedia.com/articles/active-trading/040915/how-big-data-has-changed-finance.asp.

Tropina, T., & Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. Berlín: Springer.

Loenen, B. van, Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar. The case of mapping data in the European Union. *Government Information Quarterly*, *33*(2), 338–345.

Violler, P. (2017). El Estado de la Proteccion de Datos Personal en Chile. *Derechos Digitales America Latina*. Recuperado el 28 de noviembre de 2017 de https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf.

Wehbé, A. (2017). OPM Data Breach Case Study: Mitigating Personnel Cybersecurity Risk. *Boston Public Interest Law Journal*, *26*(1), 18.