

Daniel Álvarez Valenzuela

Coordinador Nacional de Ciberseguridad

“En Chile estamos en un nivel medio de protección de datos”

Los recientes hackeos sufridos por el Poder Judicial y el Estado Mayor Conjunto, entre otros, fueron la mecha que aceleró la discusión del proyecto de ley marco sobre ciberseguridad. Una urgencia para Chile de la que conversamos en esta entrevista con uno de los principales expertos nacionales en la materia.

Por Deborah Con Kohan



Ciberseguridad. Ciberespacio. Ciberrataque. Ciberderechos.

Términos que hasta hace poco tiempo eran desconocidos, pero hoy forman parte del lenguaje cotidiano. ¡Y es que cada día las amenazas son más!, por lo que es imprescindible perfeccionar el marco regulatorio. En ese sentido, los principales esfuerzos de Daniel Álvarez Valenzuela, coordinador nacional de Ciberseguridad desde agosto de 2022, están puestos en la discusión de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, proyecto que ya fue aprobado en general por el Senado, de manera unánime, y actualmente se discute con el fin de introducirle mejoras.

Con 45 años, el interés por la computación de este abogado de la Universidad de Chile, doctor en Derecho y académico de esta misma casa de estudios, comenzó muy temprano en la adolescencia, pero su vocación humanista lo llevó a los estudios de Derecho, vinculándolos con la informática. En relación a este nuevo proyecto de ley, explica que en él se expresa la continuidad de una política de Estado implementada y desarrollada por tres gobiernos consecutivos -Bachelet, Piñera y Boric-, que dotará al país de una necesaria institucionalidad en esta materia. “Cuando exista un órgano rector de carácter técnico se podrá estandarizar, dar instrucciones generales y particulares, fiscalizar en materia de ciberseguridad”, explica Álvarez.

- El proyecto de ley sobre datos personales se viene desarrollando desde hace bastante tiempo, ¿por qué ha demorado tanto?

- Es un tema complejo. Tenemos una ley de Protección de Datos Personales del año 99, que ha sufrido al menos seis modificaciones, y se han presentado más de 120 proyectos de ley durante todos los años que lleva vigente. Es uno de los

temas donde más iniciativas existen por parte de los parlamentarios. Pero toca muchos intereses políticos, económicos, partidistas. Técnicamente es complejo y al mismo tiempo ha significado una discusión de muy largo aliento respecto a cuál es el mejor modelo de gobernanza en materia de datos personales. Hay consenso, por ejemplo, en que es necesario que exista una autoridad nacional de protección de datos personales, pero no hay consenso en quién debe ser esa autoridad.

- ¿Por quién debe ser designada esa autoridad, por el Congreso, por el Presidente o por el ministro del Interior?

- Se está debatiendo en el Congreso que esa autoridad sea el Consejo para la Transparencia o una agencia especializada, que se diferencie de un servicio público tradicional para garantizar su capacidad técnica, pero también su independencia política.

- ¿Qué sucede con la Agencia Nacional de Protección de Datos?

- También es parte de la agenda legislativa en temas de ciberseguridad, pero está mucho más avanzada. El proyecto de ley de datos personales está en segundo trámite. Uno de los puntos en discusión es cuál es el nivel de autonomía que debe tener. Hasta el año pasado la propuesta en discusión en el Congreso creaba una ley y entregaba esta atribución al Consejo de la Transparencia, que es un órgano autónomo legal, no depende del Gobierno. En cambio, las últimas indicaciones que se incorporaron en el gobierno del Presidente Piñera establecieron que la agencia sería un órgano dependiente del ministro de Economía, y eso ha sido fuertemente criticado. Si uno revisa estándares internacionales, especialmente, por ejemplo, los de la Unión Europea, se dice que la agencia debe ser



“La ciberseguridad empezó a ocupar un rol más importante en el debate público y pudimos acelerar la tramitación del proyecto de ley marco sobre ciberseguridad, logrando consensos amplios”.

autónoma e independiente. Entonces, es parte de la discusión que va a ocurrir en las próximas semanas en la Comisión de Constitución de la Cámara de Diputados.

- En su opinión, ¿qué es lo más conveniente?

- Personalmente creo que lo mejor para Chile es una autoridad de competencia mixta, es decir, protección de datos personales y transparencia. Pero si el Gobierno llega a la conclusión que el modelo de gobernanza más idóneo es el

de una autoridad autónoma sin vinculación con el Consejo, está bien, es parte de las opciones. Si uno mira experiencia comparada, hay modelos para todos los gustos, por lo que debemos abandonar los dogmatismos, también reconozco que los modelos de competencias únicas han funcionado bien.

ESCASA CONCIENCIA DE PROTECCIÓN PERSONAL

- En el último tiempo ha habido varios hackeos a instituciones públicas, como el Poder Judicial y el Estado Mayor Conjunto, entre otros. ¿Qué reacciones han motivado?

- Como sucede con todas las crisis, primero generan una sensación de inseguridad brutal y de caos, porque hay que resolver en corto tiempo un problema que no se solucionó durante mucho tiempo. Pero luego viene cómo se gestiona el incidente en el largo plazo y eso en general es positivo. La ciberseguridad empezó a ocupar un rol más importante en el debate público y pudimos acelerar la tramitación del proyecto de ley marco sobre ciberseguridad, logrando consensos amplios. Por otra parte, si uno mira lo sucedido en los últimos meses, se ve una constante en la cual hay ataques en la región. Por ejemplo, lo que le pasó al Estado Mayor Conjunto chileno, que significó la pérdida de más de 200 *gigabytes* de información, le ocurrió simultáneamente a cinco o seis fuerzas armadas de la región. Lo que le pasó al Poder Judicial, con ese *ransomware* que le capturó una cantidad importante de computadores, le había ocurrido una semana antes a varios poderes judiciales federales en Argentina. Por lo tanto, en general son oleadas que afectan a la región y ahí no nos diferenciamos mucho.

- En el caso de instituciones públicas, los ataques de ciberseguridad son

“Hoy día Google sabe mucho más de uno que probablemente el psiquiatra o el psicólogo, porque uno le pregunta cosas íntimas cuando tiene dudas existenciales”.

expuestos por la prensa prácticamente el mismo día en que suceden, no se da lo mismo en el caso de los privados.

- Sí, porque por ser pública la institución debe notificar, presentar denuncia y hacer investigación judicial y administrativa. Pero la misma semana que conocimos varios ataques del sector público, también hubo otros importantes en el sector privado. Sin embargo, como la legislación no establece para ellos obligación de notificar incidentes, pasan desapercibidos a menos que las empresas quieran cobrar algún seguro. En ese caso sí tienen que denunciar, pero hoy día las compañías que tienen seguros en temas de ciberseguridad son menos de 100.

- Las personas, en general, ¿tienen conciencia de la importancia de la protección de sus datos, o solo una vaga noción?

- Hemos transitado muy rápido desde una economía y una sociedad esencialmente analógica a otra digital, sin educación respecto del uso de tecnologías digitales. Por tanto, hoy día hablar de ciberseguridad o de higiene digital para la mayoría de la gente es chino. Pero las personas han aprendido cosas importantes, por ejemplo, por experiencia de vida, a crear una clave en el teléfono: “Si me roban el teléfono y no tienen la clave,

no van a poder acceder a los contenidos que están ahí”.

Esto implica un cambio cultural importante, ya que se busca proteger lo que está en el teléfono. Las personas necesitan entender que esa misma medida básica deben tomarla de manera mucho más robusta respecto a sus cuentas de correo electrónico, de WhatsApp, de la vida digital en general.

BÚSQUEDAS “A LA CARTA”

- Los algoritmos de internet ofrecen información personalizada de acuerdo a los gustos e intereses de cada uno. ¿Eso está bien, porque hacen más eficiente y simplifican la búsqueda, o representa una intromisión en la vida privada?

- Le pregunta a la persona idónea, porque yo tomo 50 medidas de seguridad para evitar que los sitios me rastreen en general. Y esta es una conversación permanente que tengo en mi cabeza. Por ejemplo, hace unos días alguien me dijo que estaba en su casa con unos amigos, se pusieron a hablar de autos y de repente el Instagram le empezó a ofrecer ofertas de autos.

- Es decir, lo escuchó.

- En general no escucha, sucede que estamos muy bien perfilados. Un hombre de 40 que tiene un auto desde hace tres años y empieza a hacer búsquedas, probablemente ya hizo otras en el pasado. Los grandes sitios de internet han aprendido mucho sobre cómo somos las personas, sobre nuestros gustos. Hoy día Google sabe mucho más de uno que probablemente el psiquiatra o el psicólogo, porque uno le pregunta cosas íntimas cuando tiene dudas existenciales. En algunos casos ese procesamiento de datos es tremendamente útil, para facilitar la vida, pero en otros se pueden producir abusos, uso no autorizado de la in-

formación. Para evitar la acumulación de tantos datos, hay prácticas tan sencillas como, por ejemplo, eliminar las *cookies* del computador cada vez que uno cierra el navegador, para impedir que el sistema se va alimentando continuamente.

-¿Cuál es el punto de equilibrio?

-El punto de equilibrio son las regulaciones sobre protección de datos personales. De aprobarse el proyecto de ley que está en el Congreso, las personas tendrían mayor control para poder decidir cómo, cuándo y dónde se utilizan sus datos. Mientras más datos nuestros estén circulando, mayor riesgo enfrentamos de ser víctimas de fraude, estafa, suplantación de identidad.

-¿Qué se puede decir respecto a los hackers? Algunos simplemente quieren robar, pero otros se definen como idealistas y creen estar ayudando al mundo al relevar abusos de poder sin un interés personal en ello.

-Es un poco más complejo, hay distintos niveles. Por ejemplo, está el delincuente o el que trata de sacar provecho de las vulnerabilidades de una organización. También existen activistas que buscan realizar sus acciones con un propósito altruista, que no destruyen el sistema, sino que simplemente sacan información y la exponen. Pero también hay un tercer componente de esta comunidad, que en el caso de Chile son decenas de investigadores de nivel mundial, varios cientos de personas que se dedican en su tiempo libre o incluso como parte de su trabajo académico o profesional a detectar vulnerabilidades para notificar a los responsables de manera tal que se subsane.

-¿Cómo es eso?

- Por ejemplo, en el gobierno de Chile todos los meses se reciben denuncias de

investigadores que dan cuenta de que tal sitio, tal plataforma o tal sistema tiene una vulnerabilidad que podría exponer los datos personales de usuario o de una persona. Ese ecosistema convive en distintos niveles, creemos que es algo que vamos a incluir en el proyecto de ley, ya que quienes se dedican a investigar para efectos de compartir esa información con la autoridad o con el responsable del sistema, requieren de protección legal. Estos son los llamados hackers éticos.

- ¿Personas de buena voluntad?

- En general, sí. A nivel mundial, las grandes compañías, como Microsoft y Google, cuando alguien descubre una vulnerabilidad importante, porque se dedicó altruistamente a buscarla, le pagan una recompensa. En Chile tenemos un investigador que todas las noches, desde hace muchos años, escanea toda la red chilena, de manera automatizada. Inventó un robot y todos los días analiza las diferencias entre las sucesivas noches. De repente descubre que alguien cambió la configuración de un servidor, por ejemplo de correo electrónico, para hacer una actualización, pero la actualización quedó mal hecha y el servidor abierto. Entonces ese investigador avisa las brechas de seguridad. No quiere reconocimiento, de hecho, nos ha prohibido expresamente que mencionemos su nombre. Tampoco quiere dinero, lo importante para él es el desarrollo de su capacidad técnica y prestar un servicio a la comunidad.

- Mirando el mundo del futuro, ¿cree que llegaremos a tener una especie de hermano mayor orwelliano?

-Espero que no, aunque puede ser más la expresión de un deseo que de una realidad. En general, los países están moviéndose a regulaciones donde se están restringiendo de manera más fuerte los usos de los datos de las perso-



“De aprobarse el proyecto de ley que está en el Congreso, las personas tendrían mayor control para poder decidir cómo, cuándo y dónde se utilizan sus datos”.

nas, lo que no resta que las compañías en general siguen en el afán de acumular más datos. Al menos lo que yo espero en Chile, es que el régimen de protección de datos personales permita restringir las formas en que se procesan los datos hoy día. Y a medida que vayamos avanzando y tengamos una autoridad pública vinculada, eliminemos esas distorsiones y nos alejemos de la posibilidad de que haya una sociedad de la vigilancia. 🗽