Diario Constitucional.cl
Domingo, 9 de agosto de 2020

Artículos

Santiago, 5 de marzo de 2020

Bailando solos y borrachos: El usuario y el panorama de la ciberseguridad en Chile.

Creo que la mejor manera de describir la situación del usuario en materia de ciberseguridad en Chile es mediante un personaje que podemos encontrar en la fauna de una fiesta.

Por: Pablo Lapostol

Un amigo abogado, interesado en materia de ciberseguridad, me pidió que le explicara cual era la situación actual de la legislación en materia de ciberseguridad en Chile y en qué posición se encontraban las personas frente al avance implacable de los sistemas informáticos en nuestras vidas. Esta columna es una versión mejorada de la explicación que di ante esa consulta.

Computadores en todos lados, ¿y ahora quién podrá defendernos?

La ciberseguridad la podemos definir como "la habilidad de proteger el uso del ciberespacio de ciberataques" [1] o como la disciplina que se aboca "a preservar la confidencialidad, integridad y disponibilidad de sistemas de información" [2]. No es necesario su comprensión cabal pero en el estado de la sociedad moderna la totalidad de los dispositivos electrónicos que utilizamos implementan o debieran implementar de una u otra manera requerimientos de ciberseguridad.

Nuestros dispositivos informáticos de uso cotidiano y los sistemas más críticos de la sociedad requieren de un adecuado sistema de ciberseguridad para operar de manera correcta impidiendo la interrupción de sus servicios o protegiendo la información de sus usuarios. Desde la tendencia de dispositivos "*smart*", auto, celular, refrigerador, cafetera, casas, entre otros, o sistemas más críticos como aquellos que controlan la electricidad, el agua o los sistemas informáticos de los hospitales requieren de una adecuada infraestructura de seguridad.

Una situación equivalente serían los automóviles que deben contar con cinturones de seguridad, airbags, o un diseño que permita reducir el daño de los usuarios del vehículo en caso de un choque, o que las calles y carreteras cuenten con el adecuado pavimento o señaléticas para su tránsito. Ambas situaciones se asemejan en tanto presentan ciertos riesgos de posibles daños al realizar la actividad, pero tienen una diferencia fundamental, en que los sistemas informáticos se encuentran presentes en casi la totalidad de las actividades de las personas o al menos nos acompañan a la mayoría en nuestras actividades diarias.

Esta omnipresencia de los sistemas informáticos nos ha llevado a que la ciberseguridad haya pasado a ser

una preocupación cotidiana. Bruce Schneier experto en materias de ciberseguridad describe a este proceso como el intento exitoso de las personas de colocar un computador en cada dispositivo. ¿Auto que requiere operaciones mecánicas para poder ser conducido?, agreguemos un computador, ¿el celular es un dispositivo que requiere señales para poder realizar llamadas?, convirtámoslo en un computador. El refrigerador debe tener un sistema de control para mantener la temperatura adecuada, instalemos un computador también.

La presencia de los computadores en nuestra vida es algo omnipresente, casi divino, y debiéramos pensar en la mayoría de nuestros dispositivos, en opinión de Schneier, como computadores que hacen x (siendo x la función de producto tecnológico que le es ofrecido). El celular es un computador que hace llamadas, el refrigerador inteligente un computador que refrigera, el auto es un computador que conduce e incluso su cafetera hace cálculos mejor que usted. La mejor pista para identificar esta clase de dispositivos es si es promocionado como "*smart*" o si se vincula con el logo de "*Internet of things*", aunque casi la totalidad de dispositivos tecnológicos que se ofrecen en el mercado actualmente satisfacen esta descripción, el de ser un computador que hace x.

Es este fenómeno de una presencia mayor de computadores en la vida de las personas que hace que surja la pregunta sobre cuál es la situación del usuario de estos sistemas. Si los sistemas informáticos antiguamente eran cosa de unos pocos privilegiados el panorama actual no puede estar más alejado de eso. Frente a sistemas inteligentes que registran lo que hacemos, desde el tiempo que pasamos en el celular, donde nos encontramos en cada momento, con quien compartimos, que conversamos que escribimos, surge de manera natural la pregunta de si estos sistemas son seguros.

El usuario, un bailarín solitario

Creo que la mejor manera de describir la situación del usuario en materia de ciberseguridad en Chile es mediante un personaje que podemos encontrar en la fauna de una fiesta. El ciudadano es la persona que está algo alcoholizada, y ese trance le hace creer que puede hacer todo bien. ¿Cómo estoy bailando?, fantástico piensa esa persona ¿Sera una buena idea invitar a bailar por quinta vez a la persona que ya nos ha rechazado cuatro veces?, Claro que sí. Me volvió a rechazar ¿sigo bailando solo?, pero por supuesto. Las luces apagadas de la fiesta, la fuerte música y la infusión que bebió le impiden ver de manera adecuada la realidad, y lo que está sucediendo es que es el hazmerreír de la fiesta. La gente se aprovecha de ella convenciéndola de que le compren tragos o entre en conversaciones intimas de su vida con desconocidos, las personas de la fiesta se ríen diciéndole que baila excelente para que continúe dándoles entretenimiento y solo la presencia de alguien que prenda las luces o derechamente se lo lleve de ese lugar impedirá que siga haciendo el ridículo o se haga daño. En materia de ciberseguridad quien puede evitar que siga sucediendo este pobre espectáculo es el derecho y su llegada ante el panorama antes descrito es urgente.

En Chile, a diferencia de países con legislación más avanzadas, no contamos con las herramientas legales necesarias para evitar los posibles daños en materia de ciberseguridad. Otros países cuentan con leyes especializadas que funcionarían como un amigo o grupo de amigos que evitan que las personas sufran daños o que en caso de que alguien pretenda aprovecharse de ellos los protejan. En Chile en cambio el usuario está solo y borracho. No contamos con una obligación general de reporte ante incidentes informáticos, asique es difícil saber si hacemos el ridículo. Las sanciones establecidas en la materia no emana de cuerpos legales que se dediquen a esta materia por lo que alguien se aprovecha de nuestra información o infringe nuestros sistemas informáticos las sanciones son más bien simbólicas o se derivan de cuerpos legales que se dedican a otras materia, como protección al consumidor, infracciones contractuales o sanciones que pueda imponer el órgano fiscalizador (salvo en materia financiera).

Esta situación es compleja porque Chile es uno de los países que cuenta con mayores avances en Latinoamérica en materia de acceso a internet. El número de teléfonos celulares por persona ha explotado 27 millones en 2018, el acceso a internet desde los hogares ha crecido enormemente y la promoción de internet como herramienta para las personas es algo que ha pasado a encontrarse en la discusión sobre si

constituye o no un derecho humano. Así la interconectividad y la presencia de computadores o dispositivos electrónicos conectados a internet en nuestra sociedad solo aumentara.

En este contexto los estudios a disposición que examinan el conocimiento del usuario no son alentadores y dan vida al bailarín temerario. Aunque los chilenos se muestran preocupados por la ciberseguridad la información disponible que esta preocupación no se traduce en conocimiento en la materia. Un estudio llevado a cabo por Microsoft revelo que un 89% de los jóvenes entre 14 y 15 años en Chile se consideran expertos en materias tecnológicos, pero al ser interrogados sobre en qué consiste programar un 40% señalo que era usar Excel y Word, y otro 40% señalo que era lo que había que hacer si se bloqueaba la pantalla. Básicamente se posee un conocimiento puramente instrumental Se usar el celular, sus aplicaciones y hacer llamadas, se usar el computador, programas y navegar por Internet, pero en ambos casos parte importante de usuarios denominados "nativos digitales" no comprenden cómo funcionan estos sistemas.

En los adultos existen datos similares. Un estudio que consulta sobre la operación del sistema de red 5G mostro que un gran número de ellos señalaban comprender la tecnología 5g, pero al igual que los jóvenes al ser consultados en detalle no pudieron explicar su funcionamiento. Una búsqueda (no exhaustiva) no arrojo un estudio que indicara que las personas tuvieran grandes competencias en materia de ciberseguridad. Esta es una tendencia no solo en Chile, estudios revelan resultados similares en USA y Europa. Harto acceso, harta novedad, pero poco conocimiento de la operación de estos sistemas.

Lo problemático de los estudios presentados es que nos revelan un panorama en que el pretendido conocimiento nos da una confianza temeraria, como la del borracho solitario, y hace que nos expongamos manera imprudente. No tiene sentido preguntar si ha leído los términos y condiciones de los servicios que utiliza, pero algo más pedestre pensemos en sus archivos personales ¿ha encriptado alguna vez su información personal? Si no lo ha hecho usted se encuentra, quizás, en una conversación con desconocidos a los que está compartiendo detalles íntimos de su vida. ¿Acaso ha sufrido la filtración de alguno de sus datos bancarios o de otra naturaleza (ya señalamos que en Chile no hay una obligación de reportar a los usuarios esta clase de filtraciones)? Acaban de venderle el quinto shot de tequila porque un desconocido conoce su situación e informo a otros que estaba vulnerable.

Pero uno puede imaginar una respuesta hipotética a esta situación tomando otra actividad riesgosa, por ejemplo la conducción vehículos motorizados que mencionamos arriba. ¿Cuántas personas comprenden cómo funciona el motor de su vehículo? O ¿de cómo opera sistema de conducción del vehículo? Un número menor de los usuarios debe ser capaz de responder afirmativamente estas consultas. Pero ¿qué diferencia a estas dos actividades?, acaso si no necesito saber cómo funciona el motor del auto para manejar, no será parecido en materia de Internet y computadores. Aunque hay algo de cierto en esa afirmación el punto que se debe recalcar es la diferencia en la infraestructura legal que amparan esas dos actividades.

Mientras que los automóviles cuentan con una arquitectura legal compleja, de transmisión de propiedad, control de los daños y riesgos que pueden producirse, seguros obligatorios, sistemas de responsabilidad especiales para materia automotriz, en materia de ciberseguridad el escenario es distinto. La regulación en esta materia en Chile es casi inexistente y cuando hay esta desactualizada en la mayoría de los casos. Esto unido al panorama de una omnipresencia informática produce que las herramientas dadas por el sistema legal se convierten en inútiles para dar satisfacción a los requerimientos que una sociedad moderna exige en esta materia que cada vez se expande a un mayor número de ámbitos. Sea porque no se les dan a los usuarios las herramientas para reclamar sus derechos o aquellas que se les dan son inútiles, o porque no se le exige a quienes provean servicios informáticos o deban mantener estos sistemas exigencias claras de protección de sus sistemas. Exponiendo por tanto no solo a sus usuarios, sino que a su propia actividad.

Panorama regulatorio en Chile

En Chile contamos con instrumentos de políticas públicas en materia de ciberseguridad y ciberdefensa, estos ofrecen directrices generales en esta materia como son la Política Nacional de Ciberseguridad y la Política de Ciberdefensa. Más que herramientas legales (que permitan el ejercicio de acciones indemnizatorias) estos documentos que se refieren a las políticas públicas que se están implementando o que deben implementarse y enumeran principios relevantes de interpretación para los conflictos jurídicos futuros en estas materias.

Es en este escenario en que el derecho ha de hacer ingreso (urgentemente). ¿Pero cuáles son las herramientas con las que cuenta el derecho para hacer frente a las exigencias de ciberseguridad? ¿Cómo puede enfocar su esfuerzo regulatorio? La manera en que el derecho puede hacer frente a las exigencias en materia de ciberseguridad pueden agruparse en tres perspectivas de regulación que son la autorregulación, la regulación general y la regulación específica (hay maneras más detalladas de hacer la agrupación pero para efectos de simplificar estas tres resultan más ilustrativas)

El concepto de autorregulación se refiere a la capacidad de las personas y organizaciones de regular su propia conducta, el concepto jurídico tradicional que engloba de mejor manera esta actividad es el de *lex artis*. No son normas legales en el sentido estricto del término, surgen de manera más bien convencional o mediante una estandarización de los requerimientos de la industria [3] [4]. La regulación general se refiere a normas de carácter general y obligatorio, una ley, y en la mayoría de los casos se corresponde con la ley de un tema, de ciberseguridad financiera, de protección de datos personales, de protección al consumidor, etc. Por regulación específica, esta es aquella que surge en ambientes especializados o de ámbitos en que existe una mayor regulación sea mediante la superintendencia de un órgano fiscalizador y regulador, o mediante la emisión de normas técnicas especializadas de un órgano especializado. Lo característico de ella es el detalle en la descripción de las obligaciones.

La autorregulación hasta ahora ha sido el paradigma dominante en materia de regulación (o ausencia de regulación) de ciberseguridad. Sin normas claras y generales, son las propias exigencias de operación de sistemas informáticos y las exigencias que puedan surgir de la industria en que operen las empresas y servicios las que han marcado la pauta en ciberseguridad. El ejemplo más paradigmático de esta clase de normas son las ISO/IEC 2700 en materias de ciberseguridad.

De esta situación de autorregulación hemos hecho un tránsito parcial a una en que normas generales de materias distintas a la ciberseguridad han hecho de manera indirecta presión para que se produzca una elevación del estándar en materia de ciberseguridad. Ejemplo de esta presión indirecta podemos verlo en las normas de protección al consumidor en materia de comercio electrónico o los casos de fraude informático en que se le ha exigido a los bancos la restitución de los fondos que fueron sustraídos de las cuentas de sus clientes. Para poder satisfacer estas exigencias se requieren la implementación de sistemas informáticos más sofisticados o que den más atención a la seguridad de sus sistemas. Igualmente la provisión de ciertos servicios informáticos o la mantención adecuada de los sistemas informáticos pueden llegar a constituir eventuales infracciones de contratos o pueden llegar a producir un daño generando responsabilidad civil. Por lo que la ciberseguridad y su adecuada implementación en esta clase de casos se requieren para evitar incurrir en una eventual responsabilidad por daño o por infracción contractual.

Estas son en su mayoría situaciones ajenas a la ciberseguridad específicamente pero en que la satisfacción de requerimientos avanzados en esta materia es necesario, por lo que se logran ciertos avances en estos planos.

Donde comenzamos a fallar es en las normas generales específicamente vinculadas a ciberseguridad. En Chile contamos con una ley de protección de datos personales y una ley de delitos informáticos, por lo que podría pensarse que solo bastaría la dictación de algunas normas específicas en materia de ciberseguridad para completar el panorama básico de protección informática de las personas. Pero la situación que ha sido diagnosticada por años por la doctrina es que las normas vigentes en esta materia están desactualizadas. La ley de delitos informáticos es prehistórica en consideración a los estándares de la

materia y la ley de protección de datos personales no otorga herramientas eficaces de protección a la seguridad de los datos de los usuarios, junto a otras falencias.

Ambas normas se encuentran con reformas tramitándose en el Congreso. La ley de delitos informáticos que será actualizada por la reforma y puesta al día de Chile con el Convenio de Budapest. Igualmente la ley de protección de datos personales cuenta con un proyecto de reforma en la materia que pretende elevar el estándar al nivel europeo, siendo una norma con el ADN del Reglamento General de protección de datos personales, mas coloquialmente como GDPR (con pronunciación anglo). Se encuentra pendiente de envío la ley de ciberseguridad general.

En materia de regulación específica o especializada en la materia podemos encontrar el mejor ejemplo en las normas que fueron dictadas por la SBIF (ahora CMF) de notificación y registro de incidentes informáticos. Estas son normas sumamente detalladas en cuanto a tiempo de respuesta, manera de registro, comunicaciones a realizar a los usuarios afectados, entre otras cuestiones, a diferencia de la norma contenida en la reforma a la ley de protección de datos personales que contiene una norma de lenguaje general sobre la obligación de notificación del incidente informático.

Igualmente la dictación del instructivo presidencial en materia de ciberseguridad revela una preocupación en llenar el vacío existente en la materia de ciberseguridad en el sector público, que unido a la dictación de la ley de transformación digital del Estado impondrá una mayor presión en organismos públicos de actualizar su normativa en materia de ciberseguridad al ordenar esta norma el traspaso de una gran número de procedimientos a formato digital, junto a otros decretos presidenciales en esta materia. Junto con estas iniciativas la labor llevada a cabo por CSIRT que ha comenzado a incorporar por medio del Instituto Nacional de Normalización las normas ISO en materia de ciberseguridad.

En conclusión el panorama de la regulación en materia de ciberseguridad se encuentra en movimiento, diversas iniciativas legales aún se encuentran en trámite pero continúan avanzando (hasta el día de publicación de esta columna ninguno de los proyectos mencionados se ha archivado). En materias de regulación específica se ha avanzado, especialmente en materia financiera y en el sector público. Iniciativas de educación en materia de ciberseguridad han comenzado, octubre se ha declarado “mes de la ciberseguridad”. Pero la evidencia demuestra que lo más crítico en estos momentos es la dictación de los cuerpos legales pendientes, necesarios para acompañar al usuario, que en estos momentos se encuentra solo en la pista de la ciberseguridad. (Santiago, 5 de marzo de 2020)

[1] Glosario NIST

[2] Cybersecurity Law and cases, Robert Chesney.

[3] La autorregulación y sus fórmulas como instrumento de regulación dela economía, M. Mercé Darnaculleta i Gardella.

[4] Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, Tatiana Tropina & Cormac Callanan.