OPINION SOBRE EL PROYECTO DE LEY DE DELITOS INFORMÁTICOS QUE ADECUA LA LEGISLACIÓN NACIONAL AL CONVENIO DE BUDAPEST

El 25 de octubre de 2018 el Gobierno ingresó al Congreso Nacional el proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest (el "Proyecto").

El Proyecto (Boletín N° 12192-25) se encuentra en su primer trámite constitucional y fue aprobado en general en el Senado con fecha 13 de marzo de 2019.

Desde la Alianza Chilena de Ciberseguridad[1] (la "Alianza") estimamos que el Proyecto constituye un avance importante para nuestro país en lo que se refiere a la penalización y persecución de delitos informáticos, sin embargo, existen ciertos elementos que, a nuestro juicio, todavía son mejorables o que no han sido abordados en el texto propuesto.

Este documento contiene la opinión de la Alianza Chilena de Ciberseguridad relativa al Proyecto e incluye una serie de comentarios y sugerencias, tanto generales como específicos. Se incluye, además, un apartado con antecedentes adicionales que contiene información relevante sobre la notificación de vulnerabilidades en materia de Ciberseguridad.

I. ANÁLISIS GENERAL DEL PROYECTO

1) Se recomienda establecer medidas que aborden las labores de investigación y educación en materia de Ciberseguridad y la revelación responsable de vulnerabilidades

a. Ideas iniciales

El mantenimiento y desarrollo de nuestra vida digital requiere de la coordinación cuidadosa del trabajo de dos roles en nuestra sociedad: los fabricantes de dispositivos y sistemas informáticos, y los profesionales e investigadores de seguridad. La historia y los datos muestran que los fabricantes rara vez comercializan dispositivos y programas informáticos seguros o ausentes de vulnerabilidades. Las razones detrás de esto son múltiples,

[1] La Alianza Chilena de Ciberseguridad es una organización compuesta por ACTI, la Asociación de Aseguradores de Chile, AmCham, la Cámara de Comercio de Santiago, la Cámara Nacional de Comercio, el Colegio de Ingenieros de Chile, la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, País Digital, el Instituto Chileno de Derecho y Tecnología, Chiletec, e Inacap. La Alianza Chilena de Ciberseguridad es una entidad pionera en Chile que tiene por objetivo promover, potenciar y desarrollar la Ciberseguridad y sus temas relacionados a través de la realización de actividades, capacitaciones y programas vinculados a la Ciberseguridad y al impacto en las tecnologías de la información y comunicaciones en la sociedad.

incluyendo incentivos económicos (altos recursos económicos y conocimientos necesarios para producir software y dispositivos seguros), un espectro regulatorio débil, y el hecho que las fallas de seguridad no afectan directamente a los fabricantes (constituyen una externalidad) sino sólo a sus usuarios, entre otras.

Este escenario de masificación de dispositivos y programas informáticos asociados a la falta de seguridad de los mismos son la razón de porqué los investigadores y profesionales de seguridad juegan un importante rol en la protección de nuestra sociedad y los derechos de las personas: el de ser fiscalizadores independientes de programas computacionales inseguros.

En la práctica, obtener productos y servicios seguros en el largo plazo requiere que investigadores y profesionales de Ciberseguridad se preocupen de entender y estudiar la seguridad de los dispositivos y sistemas informáticos existentes. Su trabajo minucioso y sistemático logra evidenciar vulnerabilidades las cuales, de otra manera, habrían sido ignoradas - quizás hasta el momento en que ataques maliciosos las hubieran puesto en evidencia. Son esos profesionales e investigadores quienes, motivados por el deseo de conocimiento, por cultivar una reputación sólida como profesional de Ciberseguridad, o simplemente por altruismo, detectan fallas, las notifican, y con ello permiten su corrección temprana, redundando en sistemas seguros[2].

b. El papel de la regulación y la Política Nacional de Ciberseguridad ("PNCS")

Partiendo de la base que el dueño o titular de un sistema de información tiene derecho a consentir o no a que sus sistemas sean objeto de intrusiones (accesos) de parte de terceros y los bienes jurídicos asociados a lo mismo, hay también que reconocer la realidad descrita anteriormente donde los sistemas informáticos presentes en casi todos los dispositivos que usamos contienen vulnerabilidades que pueden generar graves perjuicios a los derechos de los individuos y la sociedad. Viendo esto desde un enfoque general y pragmático, ésta realidad lleva a hacer una necesaria ponderación entre los derechos del dueño o titular del sistema susceptible de vulnerabilidades, y el bienestar de la sociedad y sus miembros que se pueden verse seriamente perjudicados por sistemas informáticos deficientes.

Una legislación que no considere el rol crucial que juegan los investigadores y profesionales de seguridad arriesga poner incentivos que reduzcan o eliminen su participación en este proceso de tener sistemas seguros. Esto puede llevar a una situación donde sistemas inseguros no son arreglados sino hasta después que las fallas hayan sido explotadas

[2] Hay quienes de hecho argumentan que los investigadores y profesionales de la seguridad cumplen un rol similar al de la prensa investigativa, en el sentido de exponer las deficiencias o fallas de quienes "detentan el poder". En el mundo de la Ciberseguridad, quien determina las características de seguridad de los dispositivos y soluciones informáticas disponibles para los ciudadanos tiene ciertamente poder.

maliciosamente, implicando finalmente un alto costo para los afectados[3]. Peor aún, la historia ha mostrado que, de contar con legislación que criminalice la búsqueda y notificación de vulnerabilidades o las actividades asociadas, los fabricantes no han dudado en usarla como amenaza en contra de los propios investigadores[4]. El riesgo de verse involucrado en una acción legal puede ser muy efectivo a la hora de acallar noticias que, aun siendo ciertas, pueden afectar la reputación de un fabricante, tales como la existencia de una falla o vulnerabilidad en uno de sus productos o servicios[5].

En este contexto, la Alianza Chilena de Ciberseguridad considera que el Proyecto debe abordar esta realidad ponderando correctamente los bienes jurídicos en juego, resguardando por un lado los sistemas informáticos de la acción de criminales, y privilegiando al mismo tiempo la seguridad de la sociedad a través de la protección y reconocimiento de la valiosa actividad de los investigadores y profesionales de seguridad informática. Este enfoque está reconocido en la Política Nacional de Ciberseguridad ("PNCS") que precisamente establece como uno de sus ejes el desarrollo de capacidades en materia de Ciberseguridad desde un enfoque multisectorial y la generación de capital humano en esta materia[6]. Por su parte, una serie medidas a corto plazo para el periodo 2017 - 2018 van de la mano en ese mismo sentido, incluyendo las número 20 y 40.

c. Sugerencias concretas de acción

- Establecer uno o varios mecanismos que permitan proteger a los profesionales de la seguridad, investigadores, acádemicos y estudiantes en la realización de laborales de investigación en materias de Ciberseguridad a través de un trabajo responsable de búsqueda y notificación de vulnerabilidades sujeta a ciertos requisitos. Un punto de

[3] Este argumento aparece explicitado en detalle en *"Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges"*, un reporte efectuado por el Centre for European Policy Studies (CEPS), Bruselas, a petición del parlamento europeo en Junio 2018. https://www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges.

[4] Existen innumerables ejemplos en la literatura, pero el siguiente es destacable. Un adolecente holandés de 18 años fue arrestado por "presionar F12" en su navegador; su crimen fue darse cuenta que la ventana resultante permitía trivialmente cambiar el precio de un ticket de tren del sistema de transporte Húngaro. Si bien no explotó la falla e inmediatamente informó a la empresa afectada (T-Systems Hungary) fue arrestado a los pocos días (aunque posteriormente liberado). Ver "Hungarian hacker arrested for pressing F12", Techcrunc.com, 25 de Julio, 2017. https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/

[5] https://www.theguardian.com/technology/2014/may/29/us-cybercrime-laws-security-researchers.

[6] En concreto, la PNCS establece en la meta letra B sobre que El Estado velará por los derechos de las personas en el ciberespacio, la "Prevención Multisectorial", que establece: *"Dado que los ciberataques y ciberdelitos pueden ser llevados a cabo por organismos estatales, grupos organizados o personas individuales y que las amenazas provienen tanto del interior como del exterior del país, la respuesta debe ser multisectorial, involucrando tanto al sector privado, la academia, la sociedad civil y por supuesto a los organismos de persecución penal, de defensa y las víctimas. Para ello, es primordial generar instancias apropiadas de coordinación, encuentro y colaboración y fortalecer significativamente las capacidades técnicas y el acceso a capacitación de los fiscales y jueces, las capacidades periciales y forenses de las policías y generar pautas de cuidado mínimas para toda la población."*

partida para abordar esto en el Proyecto puede ser modificar la regulación propuesta para el acceso ilícito y el abuso de dispositivos según se señala en la parte II de este documento. Además de esto, el Proyecto, o un eventual reglamento, debería definir claramente cuándo un reporte de vulnerabilidades ha sido (a) válidamente entregado, (b) apropiadamente evaluado, (c) correctamente resuelto y (d) adecuadamente informado[7], esto permitirá tener un procedimiento concreto y bien definido cuya ejecución correcta sea evidencia del carácter lícito de las acciones de un investigador o profesional.

- Establecer en el Proyecto u otra regulación atingente obligaciones de implementar procedimientos y mecanismos de recepción, evaluación y solución de reportes de vulnerabilidades por parte de fabricantes de dispositivos o proveedores de sistemas informáticos relevantes.[8]

- Fomentar la adopción de políticas por parte del Estado de Chile que regulen condiciones en que profesionales de la seguridad puedan legítimamente hacer investigaciones estableciendo condiciones para la revelación responsable de vulnerabilidades.

2) Se sugiere la incorporación de nuevos tipos penales al Proyecto

El Convenio de Budapest fue abierto para la suscripción de los Estados el año 2001 (el "Convenio"), cuando muchas de las tecnologías que hoy están masificadas estaban recién emergiendo. Bajo este escenario, estimamos que el Proyecto no incluye tipos penales asociados a ciberdelitos o delitos facilitados por herramientas informáticas que sí existen en otras legislaciones más avanzadas en este tema, y que se explicaría por el desfase temporal existente entre la entrada en vigor del Convenio de Budapest y el desarrollo tecnológico subsecuente.

[7] Inclusive la participación de una agencia o entidad técnica de coordinación pudiera ser recomendable. La experiencia internacional indica que los procedimientos y mecanismos de notificación son más exitosos cuando incluyen entidades de confianza e independientes dentro del proceso completo de notificación, actuando de evaluadores técnicos e intermediarios confiables. Ver: The CERT Guide to Coordinated Vulnerability Disclosure", CERT CMU/SEI, Agosto 2017, https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf, y "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure", FIRST.org, 2017, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-latest.pdf?20180320.

[8] Advertimos con preocupación desde la Alianza Chilena de Ciberseguridad que, instituciones cuya actividad son críticas para el bienestar de los ciudadanos en Chile, no tienen implementadas políticas claras de reporte responsable de vulnerabilidades. Por otro lado, existen estándares ISO para la notificación y manejo de vulnerabilidades, tales como el ISO: ISO/IEC 29147:2014 "Information technology, Security techniques, Vulnerability disclosure" y ISO 30111:2013 "Vulnerability Handling Processes". En términos de políticas públicas nacionales, Holanda provee una estrategia de notificación destacable https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

De esta forma, el Proyecto puede ser una buena oportunidad para incorporar dentro del ordenamiento jurídico nacional nuevos delitos u hipótesis no contemplados por éste, como, por ejemplo:

- Los delitos asociados a la vigilancia no autorizada mediante la utilización de sistemas informáticos

Esta clase de delitos se encuentra consagrada en el Código Penal de Estonia dentro de la categoría de delitos contra la libertad. La Sección 137 de ese código sanciona a quien observe a otra persona con el objetivo de recolectar información relativa a esa persona por alguien que no está legalmente facultado para realizar tal vigilancia[9].

- La penalización del uso de datos personales de terceros para la comisión de un delito informático

A nivel comparado, esto se encuentra, por ejemplo, como agravante en los artículos 264 y 264 bis del Código Penal español para los casos de daño informático y perturbación informática, estableciendo que las penas se impondrán en su mitad superior "cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero"[10].

3) Se sugiere abordar las tecnologías no contempladas en el Convenio de Budapest

El Proyecto no se hace cargo de los desafíos asociados a la computación en la nube – que implica almacenamiento de datos en servidores localizados en diferentes jurisdicciones; y de las dificultades que plantea en la investigación de ciberdelitos. Cabe destacar que este tema está siendo hoy tratado por los Estados participantes del Convenio de Budapest para preparar un nuevo Protocolo adicional que aborde la tecnología *cloud* y la forma de manejar la evidencia en este contexto[11].

4) Se recomienda abordar el uso indiscriminado de Bots o programas computacionales que realizan tareas automáticas y que imitan comportamiento humano

Latamente se ha discutido este último año sobre la relevancia que puede tener para el sistema democrático y económico el uso indiscriminado de Bots, y cómo estos programas

[9] https://www.riigiteataja.ee/en/eli/522012015002/consolide
[10] https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444&tn=1&p=20150428
[11] https://www.coe.int/en/web/cybercrime/-/strategic-directions-for-the-t-cy-work-in-2018-2019

computacionales pueden llegar a influir en la opinión y el comportamiento de las personas[12]. Legislación comparada ya se ha hecho cargo del uso de Bots particularmente en el Estado de California, Estados Unidos[13], donde es ilegal usarlos para comunicarse con otra persona con el objetivo de engañarla acerca de su identidad artificial con el propósito de engañar a esa persona respecto del contenido de la comunicación e incentivar la compra de un producto o servicio, o influenciar el voto en una elección[14].

Senadores de ese mismo país evalúan también legislar en la materia desde el punto de vista de su impacto en el comercio electrónico[15].

5) Se recomienda abordar los actos de índole racista y xenofóbica cometidos por medios de sistemas informáticos

La penalización de esta clase de actos ya se encuentra en el Protocolo adicional al Convenio de Budapest del año 2003[16].

6) Se sugiere mantener el delito de revelación de datos contenidos en un sistema de información

El Proyecto no contempla como delito la conducta establecida en el artículo 4 de la actual N° Ley 19.223 que tipifica figuras penales relativas a la informática. Este artículo consagra el delito de difusión o relevación de datos contenidos en un sistema de información, el cual sería recomendable mantener en nuestro ordenamiento jurídico incluyéndolo en el Proyecto[17].

7) Se recomienda establecer mecanismos de capacitación del ente persecutor y las policías

Se hace indispensable que las policías y los organismos auxiliares del Ministerio Público para la investigación de estos delitos se encuentren debidamente capacitados y actualizados en las tecnologías involucradas en estos.

---

[12] https://www.theguardian.com/commentisfree/2017/oct/16/bots-social-media-threaten-democracy-technology

[13] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001

[14] El texto oficial señala: *"It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot."*

[15] https://www.rollcall.com/news/politics/grinch-bots-christmas-toys

[16] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

[17] Artículo 4° de la Ley 19.223: *"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".*

Idéntica situación deberá ocurrir en relación al Ministerio Público, considerando que será precisamente este ente persecutor quien deberá dirigir e impartir las instrucciones a las Policías en el contexto de investigaciones sobre este tipo de delitos, o bien en delitos comunes efectuados a través de medios informáticos. Se hace necesario que los fiscales cuenten con una orientación y capacitación específica a este respecto.

Junto con capacitar, se hará necesario mejorar las tecnologías con que se cuenta para la persecución penal, bajo riesgo de que las investigaciones no lleguen a buen puerto por deficiencias sustanciales en términos de capacidad tecnológica instalada.

8) Se recomienda eliminar las referencias al término "maliciosamente" que requiere un dolo directo y presenta dificultad probatoria

Se puede evaluar si es recomendable establecer, en vez de "maliciosamente", el término "ilícitamente".

9) Se recomienda establecer una escala de penas que permitan la extradición

El Convenio y las normas en el derecho nacional establecen la extradición para aquellos delitos que sean sancionados con una pena privativa de libertad de al menos un año. Dada la calidad transfronteriza de los delitos informáticos, sugerimos revisar las penas establecidas en el Proyecto de forma de permitir la solicitud de extradiciones activas o de conceder extradiciones pasivas.

10) Se recomienda establecer la competencia de los tribunales chilenos en delitos informáticos ocurridos fuera del territorio

Los delitos informáticos tienen un componente transfronterizo relevante que debe ser considerado desde una óptica de competencia de los tribunales penales cuando estos delitos tengan efectos en Chile. En este contexto se debería evaluar ampliar la jurisdicción de los tribunales nacionales a los delitos establecidos en el Proyecto cuando ellos hayan sido cometidos fuera del Chile y hayan afectado sistemas informáticos o datos informáticos localizados en Chile. Eso debería plasmarse en una modificación del artículo 6 del Código Orgánico de Tribunales que define la competencia de los tribunales por delitos perpetrados fuera del territorio nacional.

II. ANÁLISIS PARTICULAR DEL PROYECTO

COMENTARIOS AL TÍTULO I DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

1) Al Artículo 1, sobre perturbación informática:

a. Limitación innecesaria del tipo

Este artículo penaliza la obstaculización o perturbación en el funcionamiento de un sistema informático cuando este es realizado *"a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos".* Esto deja fuera de sanción aquellas perturbaciones que sean originadas por otros medios o mecanismos, como por ejemplo, un corte deliberado de energía eléctrica y sus fuentes de respaldo pero que no tenga relación con datos informáticos, o en general la modificación maliciosa de condiciones de entorno que afecten el normal funcionamiento de los sistemas, aún cuando no exista una directa intervención en ellos.

Por otro lado, la regulación actual de la Ley 19.223 contempla en su artículo 1 la destrucción o inutilización de un sistema de tratamiento de información sin limitarlo a una causa especifica.

En virtud de lo anterior, sugerimos eliminar la necesidad que el tipo solo se configure cuando exista "*introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos".*

b. Dificultad en la aplicación de la agravante

Estimamos que la agravante sobre la *imposible* recuperación del sistema informático afectado es de difícil aplicación práctica, y plantea las siguientes interrogantes: ¿Cuándo la recuperación deviene en imposible?, o ¿Cuál es el organismo técnico capaz de determinarlo?

Una agravante con mayor aplicación práctica puede ser cuando la recuperación del sistema informático perturbado implique una inversión importante de recursos económicos o tiempo.

2) Al Artículo 2, sobre acceso ilícito:

a. Determinación de la conducta típica

La conducta tipificada en el inciso primero del artículo 2 que sanciona el "acceso indebido" es considerablemente amplia y puede:

(i) desincentivar conductas lícitas y necesarias para la seguridad de los programas computacionales, asociadas a la detección de vulnerabilidades, ingeniería reversa, interoperabilidad o "*ethical hacking*"[18], o

(ii) llegar a sancionar penalmente el acceso a un sistema informático por no cumplir los términos y condiciones de un sitio web o incumplir un contrato de carácter civil[19].

En este contexto, sugerimos agregar al tipo penal propuesto un elemento doloso que no sobre criminalice conductas ajenas al bien (o bienes) jurídico que intenta cubrir el Proyecto o, en definitiva, establecer claramente qué debe entenderse por "acceso indebido".

Lo anterior se relaciona con el inciso tercero del artículo 2 que contempla una figura agravada del acceso ilícito cuando este se realice vulnerando, evadiendo o transgrediendo medidas de seguridad destinadas para impedir dicho acceso. En este contexto, es válido preguntarse la factibilidad real de que pueda configurarse un acceso indebido sin vulnerar, evadir o transgredir medidas de seguridad y, si así fuera, cuál sería el porcentaje de acceso indebidos que estarían comprendidos en estas circunstancias. Análisis de lo anterior podría sugerir que la figura comprendida en este inciso debería entonces ser la figura base del delito de acceso ilícito y no la que está establecida en el inciso primero.

[18] Una regulación penal adecuada debe considerar que los investigadores podrían requerir para sus labores tener acceso a un dispositivo de hardware o aplicación computacional, o bien acceso remoto a un sistema informático. Es usual que un investigador acceda, modifique y altere el software de un dispositivo de su propiedad a fin de evaluar su seguridad. En el proceso de estudiar vulnerabilidades, no siempre puede obtenerse una autorización explícita para el acceso a dispositivos o sistemas informáticos por parte de un investigador. Basta considerar el caso de un investigador quien, al analizar una aplicación móvil, descubre evidencia de la potencial exposición de una base de datos completa en un servidor de acceso público. Para validar si la falla es real, el investigador tiene dos opciones: (a) notificar al propietario del servidor, o (b) intentar acceder a la base de datos. Lamentablemente, la primera opción, notificar al propietario, no siempre es efectiva pues los investigadores son frecuentemente ignorados cuando no presentan "evidencia" de la vulnerabilidad notificada o, derechamente, no existen canales de comunicación disponibles para realizar esta notificación. Sin embargo, la segunda alternativa implica acceder a la base de datos completa, aún si el investigador toma los cuidados del caso para salvaguardar la información obtenida. Claramente obtener autorización de cada uno de los potencialmente afectados sería impracticable. Esta descripción se basa en un caso real. Recientemente, se reveló que Mobiispy, aplicación que ofrece la opción de espiar teléfonos de hijos o parejas, dejó públicamente disponible su base de datos con más de 95.000 fotos, videos e información confidencial. El investigador que estudió la aplicación, por semanas intentó contactar a la empresa sin éxito. https://motherboard.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings.

[19] En Estados Unidos la *Computer Fraud and Abuse Act* que pena el acceso no autorización a un computador ha sido criticada por ser extremadamente vaga en sus términos y lo cual ha dado lugar a la criminalización de situaciones asociadas al uso de sistemas informáticos que no estaban comprendidas en el espíritu original de esa legislación. Ejemplo de lo anterior son casos donde personas han sido perseguidas penalmente por el no cumplimiento de términos y condiciones en una página web o el no cumplimiento de las políticas internas de una empresa relativas al uso de los computadoras y las páginas de internet que pueden visitar. Más información de esto se puede encontrar en: https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service

b. Características de datos o sistemas accedidos

Por otro lado, cabe destacar que ciertas hipótesis en la legislación comparada toman en consideración las características de los datos o sistemas accedidos indebidamente para involucrar una penalidad mayor. En concreto, consideran que el desvalor de una conducta de acceso ilícito es mayor cuando, por ejemplo, el acceso es a datos informáticos calificados como información clasificada en materia de defensa nacional, o cuando los datos informáticos corresponden a datos personales sensibles. Esto también es aplicable para acceso indebido a sistemas informáticos, como por ejemplo, cuando el acceso ilícito se adquiere respecto de un sistema que forma parte de una entidad calificada como infraestructura crítica. Hacer estas distinciones dota de sensatez a la norma, pues entiende que no todos los accesos ilícitos son iguales y, por lo tanto, no todos deben ser penados de igual manera.

Ejemplo de lo anterior se puede encontrar en el artículo 217 del Código Penal de Estonia que sanciona el acceso ilícito y que contempla como agravante el hecho de que se haya obtenido acceso respecto de un sistema computacional que contiene información secreta, clasificada o prescrita como de uso oficial. También establece como agravante el hecho de obtener acceso a un sistema computacional de un sector calificado como vital (*vital sector*)[20].

3) Al artículo 4, sobre daño informático:

a. Determinación del daño serio

El artículo 4 del Proyecto establece que la pena por la alteración, borrado o destrucción de datos informáticos será aplicable siempre que con ello se cause un *daño serio* al titular de los mismos. En este sentido, la norma no define los parámetros bajo los cuales deberá entenderse que existe un *daño serio* ni las condiciones para demostrarlo; lo cual, en este contexto, podría llegar entenderse como una obligación de prueba para la víctima del delito. El tipo penal debería corregirse en base al establecimiento de parámetros que entreguen al operador jurídico herramientas para determinar si el daño es serio o no.

Además de esto, podrían establecerse casos donde el legislador califique de antemano circunstancias relativas al delito que hagan estimar sus efectos como de daño serio, como

[20] *§ 217. Illegal obtaining of access to computer systems (1) Illegal obtaining of access to computer systems by elimination or avoidance of means of protection is punishable by a pecuniary punishment or up to three years' imprisonment. (2) The same act: 1) if it causes significant damage; or 2) if access was obtained to a computer system containing a state secret, classified foreign information or information prescribed for official use only; o 3) if access was obtained to a computer system of a vital sector, is punishable by a pecuniary punishment or up to five years' imprisonment."*

por ejemplo, los daños ocasionados a una empresa o una institución pública. También sería recomendable evaluar el establecimiento de circunstancias que conlleven daños especialmente serios o graves y que, en consecuencia, su comisión involucre mayor penalidad. Sugerimos en este caso, establecer que hay daños especialmente serios cuando: (i) el daño informático involucra un perjuicio pecuniario ascendente a cierto monto; (ii) el daño informático es ocasionado en el contexto de una actividad comercial ilícita o como miembro de una organización; o (iii) el daño informático perjudica el acceso a la población de bienes y servicios calificados como críticos, o afecta la seguridad nacional.

b. Titularidad del dato afectado

Por su parte, la norma establece que el daño deberá ser producido al titular de los datos informáticos alterados, borrados o destruidos, lo cual llevará en cada caso a determinar en quién es efectivamente el titular de éstos. Con la digitalización actual, la propiedad de los datos almacenados en sistemas informáticos es múltiple e intrincada, sin mencionar además que respecto a la regulación de protección de datos personales la titularidad recae sobre la persona natural a los que se refieren. En concreto, es posible que sea recomendable limitar el tipo a la generación de un daño no respecto del titular, sino más bien respecto de cualquier persona natural o jurídica que pueda aducir legítimamente un derecho en relación a los datos informáticos dañados.

4) Al Artículo 5, sobre falsificación informática:

a. Confusa redacción del tipo penal

El tipo del Proyecto difiere sustancialmente de la Convención haciendo una remisión al Código Penal y relacionándolo con la clasificación clásica de instrumento público y privado. Para evitar problemas interpretativos y de aplicación práctica sugerimos redirigir este tipo penal al señalado en la Convención que busca sancionar la generación de datos informáticos no auténticos, cuestión que no está presente en el tipo propuesto.

b. Phishing

Se debería agregar una figura específica de phishing que cubra situaciones donde se busque engañar a una persona para obtener información relevante.

Nuestra sugerencia es utilizar la normativa de Nueva York y de California penando a la persona que, por medios de un sitio web, un mensaje electrónico o el uso de Internet, solicite, requiera o tome cualquier acción para inducir a otra persona a entregarle datos personales aduciendo tener la representación de una persona, empresa o autoridad pública sin tenerla efectivamente.

5) Al Artículo 6, sobre fraude informático: Omisión de hipótesis en el tipo penal

La redacción del delito de fraude informático se aparta de lo establecido en el Convenio de Budapest que distingue claramente entre la modificación de datos informáticos y la defraudación, y que sanciona el fraude que se genera en razón de una modificación o interferencia con un sistema informático; ambas, circunstancias que no están comprendidas en el tipo propuesto en el Proyecto.

Se sugiere modificar el tipo redirigiéndolo a la regulación establecida en el Convenio con el objetivo de obtener un tipo penal robusto.

6) Al Artículo 7, sobre el abuso de dispositivos:

a. Ausencia de delitos

La figura establece que el abuso de dispositivos acontece cuando se genera la acción "*para la perpetración de los delitos previstos en el artículo 1 a 4*". De esta forma, este tipo no contempla todos los ilícitos establecidos en el Proyecto para la configuración del abuso de dispositivos, por lo que sugerimos incluir en él los delitos de artículo 5 y 6 sobre falsificación informático y fraude informático respectivamente.

b. Falta incluir hipótesis asociada a la fabricación de software malicioso

El tipo penal que contempla el abuso de dispositivos deja fuera a la persona que escribe código malicioso para cometer los ilícitos señalados en el Proyecto, o los facilita, vende o comercializa para ese fin.

La omisión anterior significa que quien desarrolla su propio código para cometer delitos estaría excluido de responsabilidad a diferencia de quien simplemente los facilita o entrega[21], lo cual carece de lógica.

c. Se sugiere aumentar la pena asociada al delito

La sanción para este delito es de pena de presidio menor en su grado mínimo[22] y multa de cinco a diez unidades tributarias mensuales, lo cual puede conducir a una limitada persecución penal en la práctica. Lo anterior, teniendo en cuenta, por una parte, que los objetos asociados requieren de conocimiento y de un esfuerzo técnico por parte de policías especializadas, y, por otra, los plazos mínimos requeridos para otorgar la extradición.

[21] El Código Penal Alemán contempla a la persona que escribe código malicioso en su legislación de delitos informáticos.
[22] De 61 días a 540 días de presidio.

d. Se sugiere modificar la redacción del artículo dado mayor claridad en que el tipo penal requiere que esos dispositivos tengan por objeto principal la comisión de los delitos enumerados en el Proyecto

Un buen investigador o profesional de Ciberseguridad debe siempre no sólo estar familiarizado con las herramientas y técnicas utilizadas por los criminales informáticos sino saber usarlas. Tal como lo saben nuestras Fuerzas Armadas, es imposible saber cómo defenderse, a menos que se conozca las herramientas y técnicas usadas por el oponente. Enseñar Ciberseguridad requiere aprender la operación, ventajas, limitaciones y ámbitos de aplicación de dichas herramientas y técnicas. En este contexto, dar mayor claridad en el Proyecto respecto a los límites del tipo penal permitirá proteger las actividades licitas de los profesionales de seguridad, académicos, investigadores, y docentes, que utilicen esta clase de dispositivos para labores educacionales o de investigación[23].

Para esto, se sugiere recurrir al artículo establecido en la Convención o en la redacción empleada en la reciente inclusión de la letra e) en el artículo 36b de la Ley 18.168 sobre comercialización de dispositivos destinados a la decodificación de señales.

7) Al Artículo 8, sobre cooperación eficaz: Límite procesal no recomendable y facultades del tribunal en la calificación de la atenuante

La cooperación eficaz es indispensable para los fiscales en investigaciones que involucran fenómenos de criminalidad compleja, como los delitos informáticos, donde existen importantes dificultades para recabar evidencia. En nuestra opinión, el límite procesal del inciso tercero (formalización de la investigación o escrito de acusación) para expresar si el imputado ha prestado una cooperación eficaz, resulta discutible en cuanto a sus beneficios, aplicación práctica y real objetivo en cuanto a la persecución penal.

La cooperación eficaz busca generar un incentivo en los imputados que están dispuestos a colaborar y, producto de ello, obtener una sanción menor: Se trata de generar un escenario en donde el imputado analice los costos y beneficios de colaborar con la investigación. Limitarlo hasta el escrito de acusación persigue incentivar la colaboración en etapas primigenias del procedimiento en clara disonancia con la orgánica de nuestro Código Procesal Penal que contempla el reconocimiento expreso de hipótesis de colaboración en etapas intermedias como en el caso del procedimiento abreviado.

[23] Un tipo penal impreciso puede criminalizar el uso de herramientas de hardware y software con fines legítimos. Si bien la redacción actual implica una participación en delitos, la sospecha o acusación de estar involucrado en la génesis de un ilícito puede significar un peso demasiado grande para los investigadores de seguridad, desincentivando el ejercicio de su profesión y la capacitación de nuevos profesionales.

Además de esto, es relevante señalar que no es recomendable limitar la calificación de cooperación eficaz solo al Ministerio Publico, pues en definitiva quien calificará o determinará la existencia de esta colaboración y la aplicación de la atenuante serán los tribunales de justicia quienes son los encargados por ley de hacerlo.

En virtud de lo anterior, se sugiere evaluar el límite temporal en cuanto a la determinación de la cooperación eficaz por parte del Ministerio Público; y (ii) establecer que la declaración de cooperación eficaz y la aplicabilidad de la atenuante será calificada privativamente por los tribunales de justicia.

8) Al Artículo 9, sobre circunstancias agravantes:

a. Tecnologías de encriptación

Utilizar encriptación de los datos enviados en nuestras comunicaciones es probablemente una exigencia básica para la mayoría de los sistemas informáticos hoy en día. Expertos en Ciberseguridad, estándares internacionales, buenas prácticas, leyes e incluso la PNCS nos recomiendan fuertemente[24] el uso de encriptación para proteger nuestros datos de robos y filtraciones[25]. La penalización como agravante en el uso de encriptación ciertamente va en contra de la tendencia global y las recomendaciones entregadas en torno a utilizar esta tecnología como mecanismo de garantizar la privacidad de las comunicaciones.

Por su parte, consideramos que la designación específica del uso de esta clase de herramienta como agravante es una técnica legislativa feble, pues se excluye otros mecanismos o tecnologías que podrían -ahora o en el futuro- igualmente obstaculizar la acción de la justicia frente a delitos informáticos. Sugerimos adoptar un enfoque neutro que, más allá de centrase en el mecanismo utilizado, se centre en el objetivo, o sea, en el acto de obstaculizar la acción de la justicia.

b. Infraestructura crítica

Estimamos que la redacción de la agravante del inciso final del artículo 9 podría ser mejorada. En este contexto, sugerimos modificar la palabra "data" por la palabra "datos informáticos" que es la definida en el artículo 14 del Proyecto. También sugerimos evaluar la conveniencia de tener esta agravante en este Proyecto o incluir una en el proyecto de ley que regule específicamente infraestructura crítica.

c. Incorporación de otras agravantes

[24] Regulaciones como la GDPR europea (https://gdpr-info.eu/issues/encryption/) o la de protección de datos médicos de EE.UU. (HIPPA, https://www.hipaajournal.com/hipaa-encryption-requirements/).
[25] https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

En legislación comparada se consideran otras agravantes asociadas a delitos informáticos que deberían considerarse en el Proyecto, tales como:

- el hecho de cometer el delito informático en el marco de una agrupación de personas;
- el hecho de cometer el delito informático en el marco de un grupo criminal;
- el hecho de que, en virtud del delito, se hayan ocasionado daños a un gran número de sistemas informáticos;
- el hecho que el delito informático haya sido promovido o financiado por un Estado; y
- que para la comisión de delito se hayan utilizado sin autorización datos personales de terceros.

Agravantes en el mismo sentido de las sugeridas se pueden encontrar en el artículo 264 del Código Penal Español.

COMENTARIOS AL TÍTULO III SOBRE DISPOSICIONES FINALES

1) Al Artículo 14, sobre definiciones: Se recomienda cambiar la disposición de los artículos

Consideramos que la técnica legislativa utilizada para disponer de las definiciones que formarán parte de los tipos penales que se describen en el Título I podría resultar confusa. En concreto, en el Proyecto primero se describen los tipos penales y, posteriormente, se definen los conceptos que los integran, los que son relevantes para entender el alcance de la prohibición. Sugerimos que estas definiciones se incluyan al inicio del Proyecto en el Título I, para facilitar el proceso de comprensión de las conductas típicas.

COMENTARIOS A LAS MODIFICACIONES AL CÓDIGO PROCESAL PENAL

<u>Comentarios generales</u>

1) Se sugiere evaluar los problemas interpretativos y sistemáticos que podría generar en el Código Procesal Penal las modificaciones propuestas

Las actuaciones investigativas del Ministerio Publico en la obtención de correspondencia y comunicaciones están reguladas principalmente en los artículos 218, 219 y 222 del Código Procesal Penal. El Proyecto busca modificar este cuerpo legal agregando un nuevo artículo 218 bis sobre "Preservación provisoria de datos informáticos", reemplazando el artículo 219 sobre "Copias de comunicaciones o transmisiones"; y modificando el artículo 222 pasándolo a denominar "Intervención de las comunicaciones y conservación de los datos relativos al tráfico".

Esta situación fue descrita por la Corte Suprema en el informe de fecha 12 de febrero que emitió en consideración al Proyecto donde indica que con la regulación propuesta no quedaría clara la división respecto de qué comunicaciones serian regidas por uno u otro estatuto. La propuesta de la Corte Suprema es establecer regulaciones separadas en el Código Procesal Penal que dividan en (i) información relativa a comunicaciones privadas; (ii) información relativa a comunicaciones públicas; e (iii) interceptación de mensajes y comunicaciones privadas.

2) Se sugiere evaluar la necesidad de generar un reglamento que facilite la entrega de datos informáticos

De acuerdo a nuestra experiencia, existe una diferencia considerable en la forma mediante la cual se da cumplimiento a la obligación de entrega de información. Lo anterior genera, en muchas ocasiones, que se deban reiterar las solicitudes para que la información sea efectivamente recibida en los términos solicitados.

En este contexto, nuestra sugerencia es que la misma ley faculte a un organismo del poder ejecutivo para elaborar un reglamento que establezca directrices básicas acerca de cómo la información debiera ser solicitada y, a su vez, cómo debiera ser entregada por parte de los proveedores.

Comentarios específicos

1) Al Artículo 16 n°1 que incorpora un nuevo artículo 218 bis al Código Procesal Penal sobre preservación provisoria de datos informáticos; y al Artículo 16 n°2 que reemplaza el artículo 219 del Código Procesal Penal en relación a copias de comunicaciones o transmisiones

a. Se sugiere expandir las categorías de empresas que pueden ser objeto de las solicitudes de preservación provisoria de datos informáticos y copias de comunicaciones o transmisiones.

Las categorías de empresas a las que se les puede requerir para estas diligencias excluyen otras entidades relevantes de ecosistema de Internet que pueden ser claves en la persecución criminal asociada a ciberdelitos. En efecto, la redacción actual del Proyecto tiene como sujetos obligados a las "empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos", dejando fuera a otras entidades relevantes, como por ejemplo, Google o WhatsApp[26].

[26] Este punto fue señalado por la Corte Suprema en el informe de fecha 12 de febrero que emitió en consideración al Proyecto.

En relación a la definición de qué empresas son aquellas que pueden ser objeto de esta clase de medidas se puede seguir lo que establece el Convenio de Budapest o la CLOUD Act de Estados Unidos. En el primer caso, el Convenio de Budapest define expresamente al "proveedor de servicios" como "toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo". En el caso de la CLOUD Act, ésta se refiere al proveedor de comunicaciones electrónicas de contenido[27].

No obstante lo anterior, la aplicación concreta de esto deberá realizarse teniendo en consideración el lenguaje que utiliza el Código Procesal Penal para referirse a esta clase de actuaciones de investigación y las empresas objeto de las mismas. En particular, hay que considerar que el artículo 218 relativo a la retención e incautación de correspondencia actualmente se refiere a "servicios de comunicaciones", y el artículo 219 que se pretende reemplazar se refiere a "empresas de comunicaciones".

b. Se sugiere establecer que las obligaciones de preservación provisoria de datos informáticos o las copias de comunicaciones o transmisiones, son aplicables aun cuando los datos se encuentren en territorio extranjero en la medida que la empresa tenga control de ellos.

El procesamiento de datos actual implica muchas veces un procesamiento de datos transfronterizo. En consecuencia, para tener una norma de ciberdelitos de aplicación efectiva, esto no debería ser impedimento para que un proveedor de servicios que preste servicios en Chile tenga la obligación de preservar y, posteriormente, entregar datos que tenga bajo su control aun cuando estos se encuentren fuera del territorio nacional.

Este es el mismo criterio que sigue el *Cybercrime Convention Committee* que representa a los Estados relación a la Convención de Budapest respecto a la aplicación del artículo 18 de la misma (T-CY Guidance Note #10 del año 2017).

c. Se sugiere incorporar sanciones

En relación al artículo 218 bis, no vemos que exista sanción alguna para la empresa en caso de incumplimiento a colaborar ni a la obligación de guardar secreto. Para esto, se sugiere que ante la omisión de colaboración y frente a la infracción a la prohibición legal de revelar ("*tipping-off*") sobre el desarrollo de la diligencia, se disponga de una figura autónoma que castigue a los infractores de dichos deberes imponiendo una sanción (por ejemplo, pena privativa de libertad y/o multa). Adicionalmente, se debería considerar que si la infracción fue cometida por una persona jurídica, las sanciones previstas pueden,

[27] Servicio de comunicación electrónica es definido como cualquier servicio que provea a los usuarios la posibilidad de enviar o recibir comunicaciones electrónicas.

además, ser aplicadas a sus directores o representantes legales que hayan concurrido dolosamente a la materialización de la infracción.

En relación al artículo 219, la única sanción señalada en este artículo en caso de negativa a la entrega de la información requerida es la solicitud de la información al representante legal y al gerente general bajo apercibimiento de arresto. En ese sentido, sugerimos la incorporación de un catálogo de sanciones en el evento que una empresa requerida no entregue debidamente la información, por ejemplo, multa y multas duplicadas en caso de reincidencia.

2) Al Artículo 16, n°2 que reemplaza el artículo 219 del Código Procesal Penal en relación a copias de comunicaciones o transmisiones

a. Se sugiere establecer que la facultad de allanamiento podrá ser procedente cuando existan antecedentes claros y suficientes que hagan estimar que la información requerida pudiera desaparecer o volverse inaccesible, o que la empresa requerida va a entorpecer la labor investigativa[28].

El texto propuesto solo permite el allanamiento cuando existe una negativa o un retardo injustificado en la entrega de información, sin embargo, hay otros casos en que podría surgir la necesidad de que el Ministerio Público acceda a la información a través del ingreso al domicilio donde se encuentren los antecedentes.

3) Al Artículo 16 n°3 que modifica el artículo 222 del Código Procesal Penal en relación a intervención de las comunicaciones y conservación de los datos relativos al tráfico

a. Se sugiere expandir las categorías de empresas que pueden ser objeto de las solicitudes de preservación provisoria de datos informáticos y copias de comunicaciones o transmisiones.

Para esto nos remitimos a lo señalado respecto al nuevo artículo 218 bis y el artículo 219.

b. Se sugiere establecer un periodo de tiempo determinado respecto del cual las empresas deban conservar los datos relativos al tráfico.

El Proyecto establece únicamente que este periodo de conservación no puede ser inferior a dos años, pero no establece un periodo máximo, lo cual puede ir en desmedro de garantías constitucionales asociadas al respecto a la vida privada, inviolabilidad de las comunicaciones y protección de datos personales. Por lo mismo, se sugiere usar un

[28] Este punto fue señalado por la Corte Suprema en el informe de fecha 12 de febrero que emitió en consideración al Proyecto.

enfoque conservador y de extrema cautela imponiendo un plazo prudente a las empresas para conservar esta clase de datos.

c. Se sugiere minimizar la cantidad de datos relativos al tráfico que deben conservar las empresas

El Proyecto establece que las empresas deben mantener: un listado y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencia de sus clientes o usuarios. El Proyecto entiende datos relativos al tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Según se puede advertir, este artículo implica un acopio masivo de información lo cual generará fuertes incentivos para que organizaciones criminales, agencias de inteligencia de otros Estados e incluso empresas busquen tener acceso a dicha información. Considerando que el sistema de acopio deberá ser accesible para el Ministerio Público y agentes vinculados a la persecución criminal en Chile con una diversidad de miembros, es extremadamente probable que el sistema sea atacado y, eventualmente, termine siendo vulnerado y los datos filtrados. Esto último podría tener consecuencias graves para el país.

d. Se sugiere incorporar sanciones

No hay sanciones respecto del incumplimiento del deber de guardar secreto que tienen los encargados de realizar la diligencia y los empleados de las empresas concesionarios de servicio público de telecomunicaciones y proveedores de Internet. En este sentido sugerimos incorporar sanción.

4) A la modificación de la Ley N° 20.393 que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho

a. Sugerimos aludir específicamente a los tipos penales aplicables a la empresa y evitar remisiones en bloque "Título I de la ley que sanciona delitos informáticos".

b. Se sugiere enfatizar que, tratándose de los delitos informáticos, la responsabilidad de las personas jurídicas se hará efectiva sólo si la conducta que genera el ilícito haya formado parte de la ejecución de las actividades, giro u operación de la persona jurídica. Lo anterior se condice con el deber de la persona jurídica de identificar las actividades o procesos,

habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de delitos. Por ejemplo, que el delito informático se haya cometido en el contexto de las operaciones o actividades económicas de la empresa, lo que exige determinar la aplicación práctica y concreta del delito (informático) teniendo en cuenta el funcionamiento de la entidad.

******

Contactos:

Alejandro Hevia

Consejero Alianza Chilena de Ciberseguridad / Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile

Email: ahevia@dcc.uchile.cl

Carlo Benussi

Consejero Alianza Chilena de Ciberseguridad / AmCham - Carey

Email: cbenussi@carey.cl

ANTECEDENTES ADICIONALES: EL ROL DE LA BÚSQUEDA Y NOTIFICACIÓN DE VULNERABILIDADES EN LA CIBERSEGURIDAD

El trabajo de los investigadores o profesionales de (ciber)seguridad es analizar los dispositivos y sistemas informáticos de (ciber)seguridad que permiten nuestra vida digital hoy. Esto incluye analizar sistemas que manejan y protegen nuestra comunicación telefónica, nuestros mensajes por internet, nuestras transacciones financieras, nuestros autos y cámaras, o incluso nuestra vida, al considerar los dispositivos médicos.

Un componente importante de la investigación en Ciberseguridad actual consiste en entender la seguridad de los sistemas informáticos y dispositivos ofrecidos por la industria. Como sabe cualquier profesional del área y ha sido ampliamente documentado, hoy en día es imposible en la práctica producir sistemas de seguridad sin fallas (denominadas vulnerabilidades), y por ello, muchos de los sistemas que actualmente utilizamos precisamente tienen vulnerabilidades. En consecuencia, encontrar fallas o vulnerabilidades tiene un valor intrínseco para la sociedad. Algunos ejemplos de vulnerabilidades encontradas son por ejemplo en sistemas anti-robos de automóviles[29], o en sistemas de encriptación de sistemas web[30], o fallas en los sistemas de pago móviles bancarios[31].

Las motivaciones para encontrar las fallas van desde búsqueda del conocimiento y la construcción de una reputación como profesional de Ciberseguridad, hasta simplemente altruismo. Un buen investigador debe seguir un proceso de notificación estandarizado[32] donde se le informa al vendedor o fabricante involucrado, y luego interactúa con él para ayudar a que dichas vulnerabilidades sean corregidas. Todo esto sin buscar compensación monetaria. Lamentablemente hay quienes no siguen este proceso y sólo buscan lucrar con las vulnerabilidades encontradas, usando dichas vulnerabilidades para actividades criminales. Por ello, es nuestro deber como sociedad fomentar y ayudar el trabajo de aquellos investigadores que facilitan su tiempo y dedicación para encontrar fallas y resolverlas positivamente.

Pero, si encontrar vulnerabilidades es un proceso difícil reportarlas lo es más aún. Recibir la noticia de una falla en uno de sus productos o servicios ciertamente complica a los fabricantes de los dispositivos y sistemas informáticos estudiados. Desafortunadamente, en vez de obtener agradecidos los reportes de vulnerabilidades, las compañías comúnmente amenazan legalmente a los investigadores involucrados. Lamentablemente, muchos de estos intentos funcionan, acallando a investigadores sin los recursos ni el interés para involucrarse en costosas batallas legales.

---

[29] https://www.nytimes.com/2005/01/29/us/graduate-cryptographers-unlock-code-of-thiefproof-car-key.html
[30] https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf
[31] https://www.eldinamo.cl/nacional/2018/05/03/hackers-revelan-graves-fallas-en-transacciones-online-del-banco-de-chile/
[32] ISO/IEC 29147:2014, ISO/IEC 30111:2013.

Pero aquí vale la pena preguntarse si mantener en secreto una vulnerabilidad es una buena idea. Si la información sobre la vulnerabilidad se mantiene secreta, no se enterarán los criminales. Este argumento se sustenta en dos supuestos. Primero, que los criminales (mal llamados hackers en la prensa) no pueden encontrar las vulnerabilidades por si solos, y segundo, que los vendedores o fabricantes de los dispositivos y sistemas gastan considerable tiempo y dinero encontrando y arreglando estas vulnerabilidades secretas. Ambos supuestos han resultado ser falsos. Los criminales han mostrado ser más que capaces para encontrar vulnerabilidades, y la historia ha mostrado que publicitar la existencia de las vulnerabilidades ha resultado ser la única razón por la cual los fabricantes parchan continuamente sus software y sistemas[33].

Las vulnerabilidades afectan a todos, no sólo a los investigadores. Si los "buenos", los investigadores y profesionales de la Ciberseguridad, no tienen permitido encontrar estas fallas y ayudar a corregirlas, entonces los "malos", los criminales, las encontrarán, explotarán y usarán para su propio beneficio en actividades ilícitas.

Los investigadores que encuentran vulnerabilidades frecuentemente siguen un proceso estandarizado de notificar o reportar los detalles a los fabricantes, interactuar con ellos para ayudar a corregirlos, y finalmente publicitar las vulnerabilidades y su solución. Pero ¿por qué publicitar del todo la información de las vulnerabilidades? En un comienzo, los investigadores luego de descubrir vulnerabilidades en dispositivos y sistemas informáticos procedían a enviar los detalles a los fabricantes. Estos típicamente los ignoraban, o incluso amenazaban con acciones legales si difundían esta información.

Como reacción, los investigadores comenzaron a publicar solamente la existencia de dichas vulnerabilidades (más no los detalles). Los fabricantes, ante esto, comenzaron a argumentar que las vulnerabilidades no eran tales, no funcionaban, o que eran "teóricas", ignorando el problema. Por supuesto, cuando luego aparecía el ataque concreto, a manos de criminales, el fabricante rápidamente procedería a parchar la vulnerabilidad, disculparse mediáticamente y concluir echándole la culpa a "los hackers", quienes con un mal uso de sus habilidades causan las pérdidas económicas de sus clientes. Sólo cuando los investigadores comenzaron a publicar todos los detalles de la vulnerabilidad (usualmente luego de un corto período de gracia donde se le da la oportunidad al fabricante para corregirla), los fabricantes comenzaron a parchar las vulnerabilidades más sistemáticamente.

¿Por qué al notificar una vulnerabilidad es conveniente definir un plazo perentorio para publicar todos los detalles? La historia ha demostrado que las empresas siempre argumentan necesitar "más tiempo" para parchar una vulnerabilidad, por lo que, de no

[33] Parte de este texto está inspirado en la excelente columna de Matthew Green, académico de la Universidad John Hopkins, Baltimore, EE.UU., donde argumenta la necesidad de eliminar las prohibiciones remanentes en la legislación DMCA norteamericana que limitan la investigación respecto a la seguridad de sistemas anti-copia. https://blog.cryptographyengineering.com/2016/07/28/statement-on-dmca-lawsuit/

mediar plazos, lo usual es que la vulnerabilidad tome mucho tiempo en ser parchada, si alguna vez lo es. Por ello, los investigadores comenzaron a definir plazos "razonables" de común acuerdo, o siguiendo o mejores prácticas internacionales de la industria. Por ejemplo, luego de notificar al fabricante, Google espera 90 días antes de hacer el reporte público, el CERT (CMU/SEI) recomienda 45 a 90 días y el INCIBE-CERT (España) recomienda 60 días si el fabricante no ha tomado las medidas suficientes para solucionarlas. Luego de ese tiempo, INCIBE emite un reporte conjunto con el investigador.[34]

[34] "Política de Reporte de Vulnerabilidades", https://www.incibe-cert.es/sobre-incibe-cert/politica-reporte-vulnerabilidades.