REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 2 (2020) • PÁGS. 1-4 • DOI 10.5354/0719-2584.2020.60658
PUBLICADO: 31/12/2020

EDITORIAL

Protección legal para la búsqueda y la notificación de vulnerabilidades de ciberseguridad en Chile

Daniel Álvarez-Valenzuela y Alejandro Hevia Angulo
Universidad de Chile

Por estos días, a fines de 2020, se discute en el Congreso Nacional de Chile el proyecto de ley que implementa el Convenio de Budapest sobre Cibercrimen y que deroga la Ley 19.223 sobre delitos informáticos de 1993.[1] Este es un proyecto largamente anhelado por la comunidad técnica vinculada a la ciberseguridad y por la comunidad científica del derecho y la tecnología, que, por largos años, ha evidenciado las insuficiencias de la ley vigente —aprobada antes de la existencia y masificación de la *web*— en múltiples conferencias, seminarios y artículos de doctrina, muchos de ellos publicados en nuestras páginas.

Entre las innovaciones que considera el proyecto de ley, queremos destacar la incorporación de normas que tienen por objeto proteger legalmente la búsqueda y la notificación de vulnerabilidades de ciberseguridad. El proyecto contempla una disposición expresa que eximirá de responsabilidad penal a los investigadores en ciberseguridad, que habiendo encontrado una vulnerabilidad en una red, sistema o programa computacional, notifiquen inmediatamente a la entidad responsable y, eventualmente, a la autoridad pública competente. De aprobarse esta norma, Chile no solo pasaría a tener una legislación moderna, sino que también de vanguardia en la región y el mundo.

Aprobar una regla de esta naturaleza sería un gran paso en la promoción del *hacking* ético y en el establecimiento de reglas legales para la divulgación responsable de vulnerabilidades.

Como nuestros lectores muy bien saben, todo sistema informático es inseguro. La tecnología actual de diseño y creación de sistemas informáticos no ha logrado produ-

1. Boletín 12.192 que establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

cir sistemas seguros desde su origen. Como ha sido ampliamente documentado en la literatura científica (Maurushat, 2013; Kinis, 2018) y en la prensa, esto no solo incluye a sistemas informáticos tradicionales, sino también a dispositivos móviles, cámaras, drones y automóviles, entre otros. Como se puede intuir, en estos días todo dispositivo electrónico lleva un computador dentro. Esto debiera motivarnos a considerar los posibles efectos de la legislación, en cuanto a incentivar o no la investigación en ciberseguridad.

Ante esto, la búsqueda, la detección, el reporte y la corrección de vulnerabilidades probablemente es el mecanismo más efectivo para mejorar la seguridad del *software*. El mecanismo consiste en una interacción virtuosa entre dos roles: el fabricante, el creador o el dueño del sistema informático, por un lado, y el analista, profesional o investigador, por otro. El primero, al carecer de los recursos o la capacidad técnica para descubrir las vulnerabilidades, depende del segundo para encontrarlas y corregirlas. Para funcionar, el proceso descansa en dos factores: la habilidad y la disponibilidad tanto de investigadores como de profesionales, usualmente externos, para examinar y reportar vulnerabilidades; y la corrección o solución de las vulnerabilidades reportadas por parte de los fabricantes (Maurushat, 2013). La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) destaca este proceso al mencionar la importancia de «establecer y ejecutar apropiadamente estructuras mutuamente benéficas, que permitan la divulgación coordinada efectiva» de vulnerabilidades (Silfversten y otros, 2018: 6). En palabras recientes del senador norteamericano Ron Wyden, «todos estamos mejor si los investigadores en seguridad son vistos como un recurso y no como una amenaza».[2]

Desafortunadamente, y como está ampliamente documentado (Kinis, 2018; Maurushat, 2013), las leyes de acceso ilícito sin salvaguardias legales para la investigación y la búsqueda de vulnerabilidades han sido usadas para intentar silenciar la investigación en ciberseguridad. Los fabricantes de sistemas con vulnerabilidades, al ser notificados, frecuentemente han recurrido a la amenaza de acción legal con el fin de silenciar a los investigadores, usualmente para proteger la reputación del fabricante o preservar su dominio en el mercado. Esta amenaza sigue presente actualmente y es fruto de controversia y litigación en países como Estados Unidos o en la comunidad europea (Pupillo, Ferreria y Varisco, 2018). En el presente, en la Corte Suprema de Estados Unidos, un grupo de investigadores del MIT arriesgan sanciones legales por haber expuesto vulnerabilidades de un sistema de votación electrónica, aun siguiendo todos los procedimientos estándares de notificación. Esta acción legal de la empresa afectada ha motivado una carta de respuesta de más de setenta destacados académicos e investigadores norteamericanos de ciberseguridad, defendiendo la in-

2. Conferencia en Voting Village de DEFCON 2020, 7 de agosto de 2020. Disponible en https://www.youtube.com/watch?v=d8lcsf510GE.

terpretación más restrictiva de la ley, la cual permite este tipo de investigación sin temor a represalias legales.[3]

Grandes empresas y organizaciones han aprendido la utilidad del proceso de notificación coordinada de vulnerabilidades. Las principales empresas de tecnología de Estados Unidos no solo toleran esta actividad, sino que la fomentan, otorgando premios económicos en un proceso denominado *Bug Bounty* (Pupillo, Ferreria y Varisco, 2018). Google, Microsoft, Facebook e incluso organizaciones como el Pentágono y la Fuerza Aérea de Estados Unidos, han tomado el liderazgo para interactuar tanto con la comunidad de investigadores como de profesionales de ciberseguridad y así fomentar su desarrollo. De hecho, los claros beneficios de esta interacción han sido argumentos recientemente esgrimidos para proveer protección legal para la investigación. Entre sus resultados y recomendaciones, un estudio de ENISA señala que es importante mejorar la protección de quienes encuentran las vulnerabilidades, «vía asegurar prácticas de puerto seguro (*safe harbour*) y salvaguardas legales para investigadores en seguridad que trabajen de buena fe en identificar y reportar vulnerabilidades» (Silfversten y otros, 2018: 6).

Si bien es cierto que la legislación comparada es débil en el sentido de carecer de leyes que explícitamente otorguen exenciones para investigación, fue precisamente este punto el señalado en un estudio llevado a cabo por el Centro de Estudios Políticos y Europeos (Pupillo, Ferreria y Varisco, 2018), el cual concluyó con recomendaciones para los Estados miembros de la Unión Europea. El estudio destaca los casos de Holanda, donde se han adoptado directivas para fomentar, encauzar y proteger el reporte coordinado de vulnerabilidades, y de Estados Unidos, donde directivas similares han sido publicadas por diversos departamentos gubernamentales (NTIA Safety Working Group, 2016). Es más, el estudio cita como su primera recomendación de política pública, después de la incorporación de mecanismos de reporte coordinado de vulnerabilidades en la ley, la inclusión de mecanismos de protección para investigadores de ciberseguridad con el fin de «clarificar su exposición y responsabilidad legal» y así «permitirles continuar con su trabajo sin temor a una persecución legal». La recomendación octava informa sobre la necesidad de actualizar las legislaciones nacionales al respecto (Pupillo, Ferreria y Varisco, 2018).

Finalmente, desde una perspectiva económica, la carencia de exenciones para la investigación en la ley arriesga ahogar al incipiente mercado de la oferta de profesionales y servicios de ciberseguridad, efectivamente sobrerregulando el mercado. En una industria de ciberseguridad en desarrollo como la nuestra, donde los profesionales están en desarrollo y la comunidad, típicamente joven, no siempre cuenta con la experiencia y madurez de países desarrollados, las normas legales también están

3. Para más información, véase Jack Cable y otros, «Response to Voatz's Supreme Court Amicus Briefable», *Disclose*, disponible en bit.ly/381FE3v.

llamadas a introducir incentivos para desarrollarla en forma profesional, buscando articular las prácticas que países desarrollados ya han identificado como exitosas.

Por esto, esperamos que el Congreso Nacional respalde las propuestas legislativas que tienen por objeto proteger legalmente la búsqueda y la notificación de vulnerabilidades de ciberseguridad, ya que la seguridad de todos y todas depende un poco de ello.

Referencias

Kinis, Uldis (2018). «From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter-RVDP): The Latvian approach». *Computer Law & Security Review*, 34 (3): 508-522. Disponible en bit.ly/2MfgZ34.

Maurushat, Alana (2013). *Disclosure of security vulnerabilities: Legal and ethical issues*. Nueva York: Springer.

NTIA Safety Working Group (2016). «"Early Stage": Coordinated Vulnerability Disclosure Template Version 1.1. National Telecommunications and Information Administration». Disponible en https://bit.ly/2Xb5Um3.

Pupillo, Lorenzo, Afonso Ferreria y Gianluca Varisco (2008). Software vulnerability disclosure in Europe. Bruselas: CEPS. Disponible en bit.ly/34YlMwt.

Silfversten, Erik, William Phillips, Giacomo Persi y Cosmin Ciobanu (2018). *Economics of Vulnerability Disclosure [Report/Study]. European Union Agency for Cybersecurity (ENISA)*. Heraklion: European Union Agency for Cybersecurity. Disponible en bit.ly/2XonF7C.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).