REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 8 NÚM. 2 (2019) • PÁGS. 1-3 • DOI 10.5354/0719-2584.2019.55827

EDITORIAL

La paz y la seguridad internacionales en el ciberespacio

Daniel Álvarez Valenzuela

Editor, Revista Chilena de Derecho y Tecnología

Desde el informe del año 2010, y en especial en sus informes de los años 2013 y 2015, el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de Naciones Unidas —mucho más conocido como el Grupo de Expertos Gubernamentales (GGE) en Ciberseguridad—, ha ofrecido un diagnóstico preciso acerca del impacto de las tecnologías de la información en la paz y la seguridad internacionales, identificando, por una parte, las nuevas amenazas y los nuevos riesgos que supone el uso intensivo de tecnologías digitales y, por la otra, proponiendo una serie de acciones y medidas que los Estados podrían implementar, conforme su propio contexto local, para hacerse cargo de esas nuevas amenazas y riesgos.

Este diagnóstico ha permitido que países como Chile hayan elaborado sus políticas o estrategias de ciberseguridad en base al conocimiento común y al amplio consenso que esos documentos representan. Políticas que consideran a la ciberseguridad como parte integrante de un sistema de protección de los derechos de las personas en el entorno digital, con un fuerte compromiso de amparo a los derechos humanos que se pueden ejercer o que pueden verse amenazados por las tecnologías digitales.

Lamentablemente, sin perjuicio que han transcurrido al menos nueve años desde el primer informe del Grupo de Expertos Gubernamentales, no contamos a nivel internacional, regional o nacional, con un registro o catastro pormenorizado de las acciones o medidas que efectivamente han adoptado o implementados los Estados miembros, más allá de aquellas sugeridas en los documentos de consenso elaborados por el Grupo de Expertos Gubernamentales. La excepción son los informes voluntarios que algunos pocos Estados han presentado en los últimos años. Resolver esta falta de información centralizada podría permitir un esfuerzo adicional por parte del sector académico, la sociedad civil y el sector privado para colaborar y solicitar a cada uno de nuestros países un mayor compromiso con la construcción de un ciberespacio libre, abierto y seguro.

En el caso específico de la aplicación de las normas del derecho internacional a las operaciones en el ciberespacio, creemos que mientras un mayor número de Estados

adopte posiciones públicas sobre la forma en que interpretan esas normas, especialmente en materia de ciberdefensa y el uso de la fuerza en el ciberespacio, otros países podrían actuar de la misma manera. La decisión de Estados como Australia, Francia y Chile, por mencionar algunos países que han hecho públicos sus documentos sobre la aplicación de las reglas del derecho internacional a los eventuales conflictos en el ciberespacio, contribuye generosamente con la paz y la seguridad internacionales. En este sentido, cabría destacar los diversos esfuerzos regionales que se están llevando a cabo para profundizar las medidas de generación de confianza para el ciberespacio.

Desde otra dimensión de la ciberseguridad, quisiera remarcar un asunto al cual hemos dedicado algunos páginas en editoriales anteriores. Varios de los países de América Latina se encuentran en proceso de implementación del Convenio de Budapest sobre Cibercrimen, instrumento de derecho internacional que refleja el estado de la discusión en materia de delitos informáticos de fines del siglo pasado y principios de este siglo, momento en el cual los procesos de notificación responsable de vulnerabilidades informáticas no estaban extendidos como ahora, por lo que el Convenio de Budapest no recoge la experiencia acumulada en los últimos quince años sobre la importante labor que realizan los investigadores en seguridad informática, usualmente denominados hackers de sombrero blanco o white hackers. Nuestros países debieran acelerar la discusión abierta sobre estos dos asuntos a fin de no criminalizar a sectores de la ciudadanía que efectivamente están contribuyendo en la construcción de un ciberespacio libre, abierto, seguro y resiliente.

Finalmente, quisiera destacar el esfuerzo que hemos realizado desde la Facultad de Derecho de la Universidad de Chile en ofrecer formación a nivel de posgrado en materia de ciberseguridad, con una mirada muldisciplinaria que comprende tanto la dimensión técnica, legal y de políticas públicas. En base a nuestra experiencia nacional, la formación en materia de ciberseguridad requiere del trabajo multidisciplinario y holistico que considere la mirada desde disciplinas tan distintas como la ingeniería, el derecho, las ciencias políticas, la planificación, la auditoría, por mencionar algunas de las más relevantes.

Esta visión nos ha permitido ofrecer programas de formación integral tanto a profesionales y técnicos que trabajan directamente en áreas relacionadas a la seguridad informática, y también, igual de importante, a las autoridades públicas y directivos del sector privado que deben tomar decisiones en estas materias. Como comunidad interesada en materia de ciberseguridad, a nivel nacional o internacional, podemos avanzar en el fortalecimiento de nuestras capacidades, pero ese trabajo será inútil si no somos capaces de desarrollar esas mismas capacidades, adaptadas según necesidades, en los niveles directivos de las organizaciones públicas y privadas que son, al final del día, quienes toman las decisiones estratégicas que impactan, positiva o negativamente, en el nivel de madurez en ciberseguridad de esas organizaciones y de nuestros países.

En nuestra experiencia, la falta de compresión sobre aspectos esenciales de la ciberseguridad a nivel de las autoridades nacionales ha impedido que varios países implementen las medidas propuestas en los diversos documentos de consenso aprobados por el Grupo de Expertos Gubernamentales. La misma falta de capacidad en el nivel directivo del sector privado ha afectado la idoneidad de las decisiones que se adoptan para hacerse cargo de los nuevos riesgos y amenazas que supone el uso intensivo de tecnologías digitales. Usualmente vemos cómo se privilegian algunos aspectos de la ciberseguridad por sobre otros, como la dimensión técnica por sobre la dimensión humana.

Como tantas veces se ha dicho, el factor humano es y seguirá siendo un elemento fundamental en cualquier estrategia que pretenda ser exitosa y las instituciones de educación superior jugamos un rol fundamental en este aspecto. Desde nuestro punto de vista, los desafíos que enfrentamos son múltiples y requieren de soluciones complejas y diferenciadas según la realidad política, económica y social de los diversos países a nivel mundial. Estas son medidas imprescindibles para avanzar en la promoción y fortalecimiento de la paz y la seguridad internacional en el ciberespacio.

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.cl).