FACULTAD DE DERECHO
UNIVERSIDAD DE CHILE

Seminario Internacional Ciberseguridad y Ciberdefensa en Chile

27.11.2015

La irrupción de las tecnologías en prácticamente todas las áreas en las que nos desarrollamos y relacionamos ha significado una revolución que no ha dejado a nadie indiferente. En la actualidad nos cuesta pensar en una vida sin las redes informáticas. En palabras de la experta en tecnología del gobierno de Alemania, Cornelia Grothe, "todos necesitamos la red como el aire que respiramos."

La digitalización, la convergencia y la globalización de las redes informáticas han producido un impacto indudable en nuestras vidas, en nuestras maneras de interactuar y en nuestras formas de trabajo. Sus consecuencias han sido sin duda beneficiosas para democratizar el acceso a la información, permitir una mayor interconexión, facilitar y agilizar los procedimientos y transparentar muchos procesos.

Cada vez más operaciones de nuestra vida cotidiana las realizamos a través de estas redes, lo que evidenciamos en el gran aumento experimentado por el comercio electrónico: según el informe “Global B2C e-commerce” en el año 2014, el mercado del comercio electrónico alcanzó una cifra de facturación de 1.907 billones de dólares, con un crecimiento del 22.9%. En el año 2015 se espera un crecimiento de un 18%, lo que llevaría al comercio electrónico a los 2.251bn de dólares.

La constante actividad que desarrollamos en lo que se ha denominado “ciberespacio” no sólo nos otorga ventajas, sino que también nos expone como país y como personas. Hace unos años, Wikileaks, utilizando las redes informáticas, publica información confidencial acerca de la situación económica en Kenia, la guerra en Afganistán e Irak, entre otras, lo que reveló el poder de éstas redes y la situación de vulnerabilidad en la que se encuentran los países en materia de defensa cibernética. Sin embargo, también dio a conocer delitos y situaciones inconcebibles que algunos podrían estimar que deben ser de conocimiento público.

En el mismo sentido, el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas de la Organización de Estados Americanos de este año reveló que un 60% de los 575 organismos públicos y privados de América encuestados, han sufrido intentos de robar sus datos, principalmente a través del conocido como *phising* (engaño para que la víctima permita el acceso de software maligno a su equipo, como los falsos emails de bancos o de correos). A su vez, se advierte que el 53% de los encuestados ha visto aumentar el número de intentos de ataques informáticos, mientras un 40% responde que se mantiene estable. Un 76% está de acuerdo en que esos ataques se están haciendo más sofisticados.

En nuestro país, se constató que sólo durante el mes de octubre del año pasado un centenar de sitios web chilenos fueron hackeados, entre ellos dominios de la Armada y la Superintendencia de Seguridad Social y sólo durante sus 20 primeros días, hubo 112 ataques a dominios nacionales, incluyendo dos sitios del Gobierno.

Estos ataques no sólo afectan a países tan grandes y que, parecían contar con una seguridad infranqueable, como Estados Unidos, sino también a empresas multinacionales con tecnología de último nivel como Sony Pictures y en nuestro país Homecenter, ambas víctimas de robo de información a través de las redes informáticas en octubre del año pasado.

Esto nos obliga a poner en la balanza el legítimo ejercicio de la libertad de expresión y de los derechos a la información y al uso de las tecnologías, por una parte, y la seguridad y privacidad de los datos personales, por la otra y a relevar la importancia de la disponibilidad del ciberespacio y la integridad, autenticidad y fiabilidad de los datos que se muestran en él.

Frente a este escenario el derecho no puede permanecer indiferente y tiene que asumir estos desafíos. Conscientes de los cambios producidos por la tecnología y las redes de información, así como del riesgo de que sean utilizados para cometer delitos, el año 2001 se firmó el Convenio sobre la Ciberdelincuencia, más conocido como Convenio de Budapest.

Este Convenio permite una colaboración entre los países para perseguir el cibercrimen y proteger la seguridad cibernética.

Con el objeto de elevar a Chile a estándares internacionales en materia de seguridad cibernética, en abril de este año, el Gobierno creó el Comité interministerial sobre Ciberseguridad, que también será una herramienta importante en esta materia.

Sin embargo, todavía nos quedan enormes desafíos que enfrentar. Tenemos que relevar el desafío que nos impone la regulación de internet tanto para el Gobierno como para las universidades, las que tenemos que asumir el rol de proveer de abogados especializados en asuntos vinculados a las nuevas tecnologías. Por otra parte, el ciberespacio se erige como un lugar que desafía las reglas del derecho internacional, ya que no reconoce fronteras de manera clara y presiona a los países a buscar nuevos acuerdos internacionales con el fin de regular fenómenos como los ciberdelitos, el ciberterrorismo y la protección de los derechos humanos en internet.

Estos desafíos también los presenta el cambio constante a que está sujeta la disciplina, ya que tal como lo manifestó el ex Ministro del Interior y Seguridad Pública, Rodrigo Peñailillo en una visita a las instalaciones de la Brigada Investigadora del Cibercrimen Metropolitana “los delitos que se realizan a través

de Internet son cada vez más complejos, y quienes delinquen a través de la red rápidamente van mutando y creando nuevas formas de cometer ilícitos".

En esta línea, tenemos que alertar que los delitos cibernéticos ya han presentado variaciones. En el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas de la Organización de Estados Americanos ya citado se advierte que están en ascenso otras variedades de cibercrimenes más inquietantes que el *phishing*: el 40% de los encuestados afirma que se ha encontrado intentos de inutilizar sus ordenadores; el 44% ha visto intentos de borrado de archivos y el 54% ataques para manipular sus sistemas. Lo que advierte un cambio en la tendencia existente: se pasa del "simple" robo de información al sabotaje o incluso destrucción de sistemas clave.

Esto obliga a revisar continuamente nuestra legislación y nuestros mecanismos para responder con rapidez y eficacia a las nuevas amenazas que van surgiendo. El rol de la academia en este sentido es fundamental y como Facultad de Derecho de la Universidad de Chile, tenemos que generar las instancias para alertar las debilidades y falencias de nuestras normas. A su vez, tenemos que relevar la necesidad de avanzar hacia una discusión multidisciplinaria en materia de ciberespacio, donde se aborden las necesidades regulatorias desde una perspectiva que considere, por una parte, la opinión técnica provenientes

de las disciplinas de la ingeniería, las ciencias políticas, las relaciones internacional, y por cierto, el derecho.

En este sentido, tenemos que relevar el rol que cumple el Centro de Estudios de Derecho Informático de esta Facultad de Derecho de la Universidad de Chile, como centro especializado en la regulación de nuevas tecnologías, con más de 20 años de experiencia en investigación y formación especializada, tanto en pregrado como postgrado y que tiene una misión fundamental en el estudio e investigación de estos temas.

Es por esto que celebramos la organización de este Seminario Internacional de Ciberseguridad y Ciberdefensa en Chile, el primer seminario internacional realizado en nuestro país sobre esta materia y que ha sido fruto del esfuerzo conjunto de nuestro Centro de Estudios en Derecho Informático y la Subsecretaría de Defensa, la Subsecretaría de Interior y Seguridad Pública y la Subsecretaría de Relaciones Exteriores, lo que demuestra el compromiso de estas Subsecretarías y de esta Facultad con una Política Nacional de Ciberseguridad para Chile, en la que está trabajando el Gobierno.

En este Seminario se analizará la ciberseguridad en un contexto global y local, de manera que podremos advertir los distintos problemas y desafíos que se nos presentan y contrastar estos dos contextos. Enseguida, se abordará la Seguridad internacional en el ciberespacio, lo que nos permitirá

tener una perspectiva acerca de la forma en que está siendo enfrentado este tema en materia internacional. Otro tema fundamental es, sin duda, la Cooperación del sector público y privado en Ciberseguridad, que también será tema de este Seminario y que reviste sumo interés, ya que los distintos expertos en estos temas son contestes en señalar la importancia de que exista una colaboración entre ambas entidades, de manera que fortalezcamos y trabajemos en conjunto para lograr una mejor seguridad cibernética. Finalmente, este Seminario nos invitará a reflexionar sobre los desafíos de la adhesión de Chile al Convenio de Budapest para el Cibercrimen.

Estoy convencido de que tanto los temas abordados en este Seminario, como las discusiones a que darán lugar contribuirán a un mayor desarrollo de la cooperación internacional, así como de herramientas para combatir el cibercrimen y reforzar la seguridad y defensa cibernética.

Muchas gracias