TIPS Trabajos de Investigación en Políticas Públicas
Departamento de Economia . U. de Chile
N°16
SEPT. 2013

CONTENIDO

América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?

Septiembre, 2013
María Eugenia Rodríguez Florez

RESUMEN

El Estado tiene la responsabilidad de impulsar y facilitar el desarrollo basado en las Tecnologías de Información y Telelecomunicaciones (TIC's), y también garantizar una efectiva y transparente protección a los ciudadanos. Es por ello que, para hacerle frente al impacto que han tenido las TIC's y el surgimiento de un nuevo espacio virtual o ciberespacio, -caracterizado por la inexistencia de fronteras geográficas-, que se hace necesario actualizar las legislaciones para que se normen las relaciones entre las TIC's y el delito; distinguir entre tipologías de delito ***con*** y ***en*** las TIC's y crear agencias de cooperación internacionales, pues estos crímenes generalmente involucran a más de un país (donde se realiza la acción y en donde se materializa el daño).

Esto requiere modificar las legislaciones que rigen cada país de forma armonizada y crear sistemas que permitan la detección, investigación y persecución de los probables delitos en un marco que resguarde los derechos de las personas y que a la vez disminuya el riesgo de que se usen las redes informáticas y la información electrónica en contra de la confidencialidad, integridad y disponibilidad de dichos sistemas.

La relevancia de legislar de forma armonizada lo que se hace en la red, es una realidad que se impone con fuerza a medida que se expanden la frecuencia y los usos del llamado ciberespacio. Pues al ser un espacio con una dinámica propia, compleja y desconocida para la mayoría de sus usuarios, pero amigable, versátil y bondadoso en sus aplicaciones, se tiende a subestimar e ignorar los potenciales daños que puede causar el mal uso o abuso de un espacio intangible en la cotidianidad de los ciudadanos.

AUTOR
María Eugenia Rodríguez Florez es Economista de la Universidad Central de Venezuela y Magíster en Políticas Públicas de la Universidad de Chile. (maruge@gmail.com)

TIPS es editado por el Departamento de Economía de la Universidad de Chile.

El Editor Responsable es Andrés Gómez-Lobo (agomezlo@econ.uchile.cl).

POLÍTICAS PÚBLICAS
UNIVERSIDAD DE CHILE
DEPARTAMENTO DE ECONOMÍA

TIPS
Trabajos de Investigación en Políticas Públicas
Departamento de Economia . U. de Chile

"Esa es la gran ironía de la era de la información,
las tecnologías que nos permiten construir y crear
son las mismas que utilizan aquellos que destruyen y perturban el orden.
Es una paradoja que vemos cada día"
Pdte. Obama, 2009

INTRODUCCIÓN

Las tecnologías de información han creado una red que transciende las fronteras geográficas y que permite el flujo prácticamente incontrolado de datos. Sus usos y usuarios se han expandido, convirtiendo al ciberespacio en un lugar cada día más real. Esto ha impuesto la necesidad de normar las actividades que allí se realizan generando uno de los mayores desafíos de la época: *garantizar el resguardo y el ejercicio de los derechos y libertades fundamentales del ser humano, enfrentando el anonimato de la red*.

En el presente trabajo, se hace un esfuerzo por explicar qué es cibercrimen y por qué representa una amenaza para todos. Se menciona también cual ha sido la respuesta de la comunidad internacional y las prácticas de la región en la materia, destacando sus principales debilidades. Se esboza la discusión del choque de intereses que genera este tipo de regulaciones y el *trade-off* que se presenta entre el ejercicio de las libertades individuales y la protección de las mismas por parte del Estado. Para finalizar, se destaca la necesidad de diseñar estrategias coordinadas que asuman y enfrenten esta compleja y dinámica realidad a favor de evitar que la ausencia de legislación incentive la proliferación de estos delitos, convirtiendo a la región en "paraisos de impunidad".

¿QUÉ SE ENTIENDE POR CIBERCRIMEN?

El cibercrimen es un término que carece de una definición universalmente homogénea y aceptada por los especialistas en el área. Si bien muchos investigadores están de acuerdo en que es una actividad ilegal realizada a través del computador existe un desacuerdo con respecto al lugar en el que se ejecuta (Chung et al., 2004). Algunos ejemplos de estas divergencias son las siguientes definiciones:

- Chung et al. (2004): actividades ilegales realizadas a través de computadores que a menudo tienen lugar en las redes electrónicas globales.
- Parker (1998) afirma que es el sistema de información que sirve de canal.
- Philippsohn (2001) considera que se realizan a través de internet.
- Power (2002) lo asume como la intromisión sin autorización de un computador

Chawki (2005), indica que el computador tiene varios roles en el cibercrimen, pues sirve de objeto, sujeto, herramienta y símbolo. A su vez, sostiene que se diferencia en cuatro formas de los llamados crímenes territoriales: permiten un fácil aprendizaje de cómo realizarlos; requieren pocos recursos en comparación con el daño potencial que pueden ocasionar; pueden ser cometidos en una jurisdicción sin necesidad de estar físicamente presente y frecuentemente no son claramente identificados como ilegales.

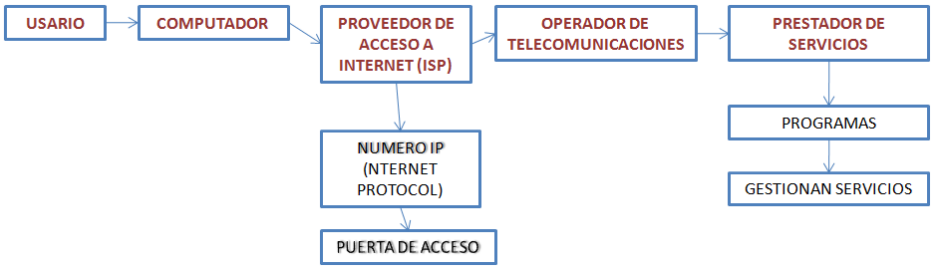
Por su parte, Kleve, De Mulder y van Noortwijk (2011) señalan la importancia de investigar el cibercrimen toda vez que es necesario conocer cómo opera a favor de diseñar las investigaciones criminales; por la percepción de que las leyes convencionales no aplican a éste tipo delitos, ya sea por no estar explicitas o por la forma en que se interpreten, y por la insuficiencia de un manejo seguro de la infraestructura que ofrece internet. Enfatizan en que este tipo de delitos dependen del conocimiento, en lo que sucede dentro de un sistema automatizado y cómo se estructura, beneficiándose

además de un vacío en la legislación dada la posibilidad de que la autoridad del Estado pueda estar indeterminada en dicho espacio.

LA INVESTIGACION: LIMITACIONES E IMPLICACIONES

Internet está constituido por un extenso número de ordenadores conectados entre sí que forman la red de redes. En el siguiente gráfico se indica el funcionamiento de la red, con el objetivo de ofrecer un mejor entendimiento de los retos que impone el cibercrimen a la investigación criminalística (Salon, 2005)

Figura 1: Funcionamiento de internet



Fuente: Delito Informático y su investigación (Salon, 2005)

Elaboración Propia

Para ingresar a la red y hacer uso de ella es necesario contar con un ISP que funciona como una puerta de acceso a internet y que asigna a cada computar un identificador único conocido como número IP. Estos números IP son un grupo de números naturales que van del 0 al 255 y que permiten una combinación aproximada de 4.000 millones de números. Para ordenadores con diferentes sistemas operativos se diseñaron protocolos de comunicación que se deben respetar para permitir que todos se entiendan. Dichos protocolos establecen que las comunicaciones son fraccionadas, lo que implica que la información es encapsulada en capas o paquetes con capacidad limitada y estandarizadas. Dichos paquetes contienen los *datos de tráfico* que son los datos de origen y destino y las IP's de origen y destino, que si bien permiten identificar los computadores involucrados y el ISP, no permiten ver el contenido del mensaje ni ubicar a los usuarios que emitieron y recibieron el mismo (Salon, 2005).

Salón (2005) sostiene que la investigación de delitos informáticos enfrenta muchas limitaciones ya sea por la ausencia de conocimientos técnicos básicos, medios de investigación definidos y el anonimato que permite la red. Pero además destaca la conservación de los datos de tráfico por parte de las ISP (lo hacen por un número mínimo de días ya que implica costes de almacenamiento y gestión de búsquedas); identificación de los usuarios (la proliferación de equipos a disposición de una pluralidad de usuarios sin ningún control); cesión de los datos a los institutos encargados de la investigación (pueden contradecir las leyes de propiedad de datos); el registro domiciliario, que implica tener un protocolo que identifique cuando es necesario intervenir un sistema informático para buscar pruebas incriminatorias y la virtualidad de las pruebas (el implicado puede autoinstalar software troyano).

Cárdenas (2008) sostiene que la mayor complejidad que enfrenta la investigación es la baja probabilidad que existe en cuanto a su detección, persecución y esperanza de castigo. Además destaca que los sistemas judiciales tampoco han hecho lo mejor en cuanto a desarrollar ajustes que le permitan salvaguardar ciertas garantías fundamentales (como el derecho al debido proceso). Pues al ser el ciberespacio un espacio sin ley, conlleva a múltiples pretensiones punitivas por un mismo hecho, lo que aunado a la dificultad de asegurar un espacio en el que impere el derecho en la práctica, daría por resultado un menoscabo de los derechos del implicado, por lo que para evitar esto, se hace necesario determinar el

lugar en que se considerará cometido un delito en internet para impedir que el "sospechoso" sea culpado y/o condenado por un mismo acto en diferentes países y bajo diferentes criterios en el proceso y en la sanción.

Chung et al. (2004), señalan que hay mucho trabajo pendiente ya que las formas convencionales de identificar a los autores del crimen, como huellas dactilares y ADN, no funcionan en este tipo de crímenes por lo que destaca la necesidad de desarrollar estudios que permitan reconocer a los autores con las evidencias electrónicas.

LA JURISDICCIÓN DEL CIBERCRIMEN

Reidenber (2005) afirma que la jurisdicción sobre las actividades de internet se ha convertido en el principal "campo de batalla" de la lucha por establecer el Estado de Derecho en la Sociedad de la Información. Brenner y Koops (2004) destacan que el asunto más difícil al momento de definir la jurisdicción es que no está claro qué es lo que la constituye: el lugar donde se cometió el acto y donde se evidenció el daño, el país de residencia del atacante y el de la víctima o todas estas razones. La jurisdicción ya no puede estar asociada al concepto de territorio, pues en cualquiera de sus interpretaciones, puede generar controversias de variada índole.

Economic and Political Weekly (2005), a través de un corresponsal especial[1], identifica las siguientes corporaciones[2] como las responsables de la "gobernanza" en internet:

- Internet Corporation for Assigned Names and Number (ICANN)[3], que tiene un manejo centralizado de los Domain Name System (DNS).
- Internet Assigned Number Authority (INAN), que asigna los números de acuerdo a una jerarquía geográfica
- Internet Engineering Task Force (IETF)[4], que es la principal responsable de desarrollar los estándares y protocolos de la red.

Mención especial merece el rol que juega National Transport and Information Administration (NTIA) del Departamento de Comercio de EEUU, ya que las decisiones de ICANN deben ser supervisadas por ésta. Adicionalmente, juegan un importante papel las empresas que manejan los servidores raíz y los llamados dominios tops .com y .net, como Microsoft y Google las cuales han sido acusadas de tener ventajas comerciales desleales bajo el temor de que puedan ser usadas por el gobierno norteamericano con fines estratégicos.

Economic and Political Weekly (2005), sostiene que si bien es cierto que la actual organización ha funcionado bien, dando evidencia de su competencia para responder a los retos que ha impuesto el boom de internet, destaca que los cambios se deben hacer no por un descontento en el funcionamiento sino por una necesidad que descansa en lo inadecuado que resultará el sistema actual en un futuro, ya que alterará profundamente los fundamentos del comercio y las ventajas competitivas de las empresas, ocasionando una mayor resistencia a cualquier acción de control gubernamental.

Sin embargo, en marzo 2010, los senadores Kristen Gillibrand y Ollin Hatch, introdujeron una iniciativa de Ley que le da a Estados Unidos el papel rector de la ciberseguridad mundial, permitiéndole ofrecer asistencia global en la identificación de amenazas y exigiéndole al presidente Obama retirar la ayuda y recursos a los países que se nieguen a hacerse cargo de la ciberseguridad. Adicionalmente, el gobierno norteamericano, para dar *transparencia y comunicación a sus procesos* puso a disposición del público *The Comprehensive National Cybersecurity Initiative,* que considera doce iniciativas, entre

[1] No suministran el nombre del autor.
[2] Reflejan la historia de internet, que surgió como un experimento del Departamento de Defensa de EEUU.
[3] Una corporación sin fines de lucro ubicada en California, EEUU. Adicionalmente, estas corporaciones enfrentan nuevos retos, por ejemplo, ofrecer caracteres no latinos para países como China e India.
[4] Asociación voluntaria de profesionales que trabajan por consenso.

las que destacan el manejo de la red federal como una red segura, la implementación de un sistema de detección de intrusos, planes de Investigación y Desarrollo (I&D) ampliación de la educación cibernética e implementación de sistemas de contrainteligencia.

LOS DESAFÍOS DE REGULAR EL CIBERCRIMEN

Salom (2005) sostiene que la Sociedad de la Información ha sido una revolución sociocultural caracterizada por una alta dependencia tecnológica, que usa Internet como un vehículo de transmisión e intercambio de todo tipo de información, lo que la convierte en un escenario para potenciales desarrollos de comercios y servicios complementarios, cuyo límite es la imaginación humana y que precisará de un importante esfuerzo para controlarlos o normarlos. Indica que la Red no contempló en su origen la necesidad de establecer parámetros de seguridad para los servicios a los que luego se destinaría, dejando el medio, los protocolos y software utilizados vulnerables a las exigencias de confidencialidad, integridad y disponibilidad que hoy se requieren.

Chawki (2005), argumenta que el incremento del uso de computadores interconectados a la red global está destruyendo la relación entre ubicación geográfica y el poder de los gobiernos locales para controlar el comportamiento online, los efectos del comportamiento online en los individuos y las cosas, la legitimidad de los esfuerzos de los gobiernos locales para lidiar con éste fenómeno global y la habilidad de contar con una ubicación física para dar aviso de las normas que rigen. Salom (2005) destaca que al convertirse en un reto intelectual para algunos y en una barrera para otros, ha generado vacíos legales entorno a la Red que afecta todos los ámbitos del derecho pues no se ha logrado unir los ámbitos tecnológicos y jurídicos, por lo que se requiere una armonización legislativa a nivel global.

A nivel internacional existe un consenso que acepta que la rápida expansión (en usos y usuarios) de internet excede las capacidades de las regulaciones, lo que crea un espacio para abusos y crímenes (espacios anónimos y vulnerables). También se reconoce que el gran reto es saber exactamente cómo hacer esto, ya que el ciberespacio ofrece tres grandes ventajas para quienes realizan actos delictivos en él: la anonimidad, la capacidad de actuar de forma individual (no impone la necesidad de asociarse) y 233 países con conexiones a internet para escoger. Un ejemplo de esto ha sido el comentario del Presidente Obama, en una rueda de prensa en la Casa Blanca en 2009, quien expresó: "El ciberespacio es real, como son reales los riesgos que conlleva". Por su parte, Schmidt (2010) afirma que a pesar de que el Presidente Obama considera la ciberseguridad como uno de los desafíos más serios de la economía, admite que como país no están preparados de forma adecuada para hacerle frente.

¿PARA QUIÉNES REPRESENTA UNA AMENAZA?

Speer (2000) argumenta que el cibercrimen es una amenaza reciente y muy diferente a las que enfrenta la seguridad mundial lo que impone la necesidad de actualizar las estructuras institucionales existentes. Su naturaleza inexacta y heterogénea se conjuga en una dinámica compleja que involucra un extenso número de actores relacionados simultáneamente en diferentes sectores. Algo que ha caracterizado la evolución del cibercrimen es que ya no solo se trata de personas individuales (o pequeños grupos) que prueban su conocimiento técnico a través de infecciones masivas y búsqueda de dinero rápido. Actualmente, son grupos de crimen organizado y especializados, con focos específicos cuyos objetivos son el control de internet y la extorsión.[5] Por ejemplo, en Brasil durante el 2013 se ha incrementado la frecuencia del secuestro y solicitud de “rescate” de las máquinas de los usuarios, utilizando el “Ransomware” un ataque (cifra y bloquea el acceso al sistema y a los archivos) que se instala una vez que el usuario ha abierto un mail de pishing o ha visitado una web maliciosa. Investigaciones indican que la solicitud de rescate puede alcanzar los 4.000 USD.[6]

[5] Tomado del Informe sobre el Cibercrimen 2008, elaborado por S21sec.
[6] Disponible en http://tecno.americaeconomia.com/noticias/aumentan-ataques-de-ransomware-en-america-latina

Este tipo de actos representan violaciones a los derechos y patrimonios de particulares, amenazas a la gobernabilidad y estabilidad de los gobiernos, generan pérdidas económicas e incentivan el desarrollo de negocios clandestinos que cazan rentas por medio del robo de información. Fernández (2007) menciona las principales formas de perjuicios patrimoniales como los spyware o archivos espías, phishing, pharming, dialers y fraudes en operaciones de comercio electrónico.

Chawki (2005), en cambio, afirma que no se cuenta con estadísticas válidas sobre la frecuencia, tamaño y pérdidas que ocasiona el cibercrimen, ya que las organizaciones que realizan las encuestan tienen diferentes definiciones y por ende ponderaciones del fenómeno. Sukhai (2004) sugiere que la subdeclaración de este tipo de delitos dificulta la acción contra los delincuentes cibernéticos ya que refuerzan la idea de que no es necesario denunciarlos dada la limitada capacidad de las autoridades de enfrentarlos de forma efectiva, además del temor que pueda surgir en las empresas de hacer pública alguna vulnerabilidad. Sin embargo, la Unión Europea indicó que el cibercrimen en el 2009 representó en costos 750.000 millones de Euros, lo que equivalía al 1% del PIB comunitario. Y según "State of the Net Survey Consumer Reports 2009" los fraudes por internet a nivel mundial estimados oscilaban en aquel entonces por los 8.000 millones de dólares.

A continuación se presentan algunas formas en que se materializan dichas amenazas de acuerdo a los actores:

- **Gobiernos**

Los Estados han fortalecido su red institucional por medio del uso de las TIC's, desarrollando el concepto de *e-Government,* que de acuerdo a la OCDE, se expande del uso de las operaciones internas para incluir la prestación de servicios electrónicos llegando a considerarlo no como un simple mecanismo que suministra información en línea, sino como un medio de interacción entre el gobierno y la sociedad.

Quizás por ello es que cada vez son más frecuentes los ataques a las páginas de los gobiernos, ya sea como medio de denuncia o de respaldo a la libertad de expresión, internet libre, entre otras causas. Un ícono de acciones es Anonymous, seudónimo utilizado por ciberactivistas que se han atribuido el hackeo de páginas oficiales de diferentes gobiernos a nivel mundial. América Latina no se ha eximido de estos "ataques"; en Perú en el aniversario 192 de su independencia, hackers borraron parcialmente páginas oficiales como forma de protesta al sistema judicial peruano. También se puede mencionar el ciberataque masivo realizado en julio 2013 a las páginas de gobernaciones, ministerios y alcaldías de Venezuela en dónde se exigía la renuncia del presidente Nicolás Maduro por considerar su presidencia como fraudulenta. Entre sus actuaciones también destacan las ocurridas en enero 2013 en Argentina cuando hackearon la página del Instituto Nacional de Estadística y Censos (vale destacar que en el 2012 ya habían derribado las páginas del Ministerio de Economía y del Banco Central), y en México cuando colocaron un manifiesto del Ejército Zapatista de Liberación Nacional en la página de la Secretaría de la Defensa Nacional.

Estas acciones también pueden ser consideradas como "simples saboteos" para demostrar la vulnerabilidad de los gobiernos en el ciberespacio o como "acciones desestabilizadoras" que "alertan" o promueven anarquía, ya sea robando información o usándola en contra del sistema. Un ejemplo de esto fueron los ataques dirigidos contra decenas de páginas del Gobierno y empresas en Corea del Sur y Estados Unidos en julio 2009. Aún se desconoce el origen y los autores, pero se estima que fueron lanzados de 16 países diferentes, entre ellos la misma Corea del Sur, Corea del Norte, Estados Unidos, Japón y Guatemala.

Sin embargo, el ejemplo más emblemático a la hora de evidenciar la vulnerabilidad de los gobiernos ha sido Wikileaks que, como se autodefine, es una organización sin fines de lucro dedicada a ofrecer noticias e información al público garantizando la anonimidad de sus fuentes. ¿Las repercusiones? Escándalos políticos y empresariales que vinculan a importantes figuras de la vida política y económica. Mercedes (2011) califica que Wikileaks puso en evidencia toda la problemática de la credibilidad (como espacio de confianza y accesibilidad) de los distintos agentes políticos y sociales de

la sociedad mundial, situación que considera delicada ya que a su juicio la credibilidad es la fuente motora de los principios democráticos.[7]

- **Empresas**

De acuerdo a Kaspersky Lab (2011), para los próximos diez años el cibercrimen se caracterizará por el aumento la demanda de espionaje comercial, robo de bases de datos y ataques a la reputación de las empresas. 2008 Data Breach Investigations Report, realizó 500 investigaciones forenses en base a 240 millones por ataques en registros vulnerados, y revelaron que el 66% de las empresas que han sido víctimas de ataques cibernéticos perdieron información que no sabían que tenían; el 73% de los ataques provinieron de fuentes externas y 18% fueron causados por gente interna; el 75% no fueron detectados por la empresa víctima sino por un tercero y que el 42% de los ataques analizados se efectuaron a través de un acceso remoto.

Por su parte, la OCDE en el informe sobre Malwares del 2007, hace énfasis en la vulnerabilidad que tienen la economía de internet y las economías locales ante el "boom" de ataques de software malicioso (que según la empresa ScanSafe se habían incrementado en 400% ese año), ya que esta situación puede afectar la confianza de los consumidores, disminuyendo su disposición a realizar diferentes transacciones por esta vía, lo que impone a las empresas la necesidad de realizar esfuerzos por crear una cultura que prevenga este tipo de actos de manera de evitar robos de información que se traduzcan en mermas de ingresos por la pérdida de productividad y confianza de sus clientes.

- **Particulares**

El aumento y uso intensivo de redes sociales[8] como Facebook, Twitter, MySpace y Hi5 no solo ha ofrecido una herramienta para estar en contacto con amigos y familiares, sino que han servido para informar de forma masiva lo que ocurre en el entorno de los usuarios. Entre sus usos y abusos[9] destaca la violación a los derechos de intimidad[10] e imagen, robo de identidad, la promoción de pornografía infantil, la trata de personas y el ciberacoso (bullying). Un ejemplo de éste último, que encendió el debate sobre si el ciberbullying debería ser un delito penado por la ley, es el caso de la joven canadiense (Amanda Todd) de 15 años que se quitó la vida en octubre de 2012 y que durante el mes previo realizó un cortometraje narrando con escritos en cartulina los abusos que decía haber sufrido.[11]

La encuesta realizada por Opera Software (enero 2011)[12] a 3.000 ciudadanos de Estados Unidos, Japón y Rusia, reveló que sufrir una violación de los datos en la red es la segunda mayor preocupación de los estadounidenses, que al 35% de los estadounidenses le preocupa que el gobierno pueda acceder a sus actividades en la red, que el 33% de los japoneses les inquieta la seguridad del comercio online y que al 38% de los rusos les inquieta la seguridad en las redes sociales.

---

[7] Disponible en: http://www.pciudadana.org/detalle/opinion/wikileaks:_consecuencias_sin_consecuencias_-1272

[8] De acuerdo a Tendencias Digitales, el 71,2% de los latinoamericanos usan redes sociales.

[9] Hasta el cuerpo humano y la salud de las personas podría verse comprometida. Pues el hacker Barnaby Jack, antes morir y de poder revalar la forma de hacerlo, demostró que podia hackear un marcapaso a 10 metros de distancia. Por lo que la posibilidad de que alteren equipos medicos como forma de agresión o extorsión en un futuro llega a ser bastante realista.

[10] Ni Mark Zuckerberg fundador de Facebook se ha eximido de esto. En agosto de 2013, el programador palestino Shreateh violento la privacidad del perfil del Zuckerberg para demostrarle al equipo de Facebook un defecto en el mecanismo protector de la plataforma y así cobrar la recompensa de 500 USD que da la red social a quien les expone las fallas del sistema. Dado que su recomendación fue ignorada por el equipo de Facebook, Shreateh decidió dejarle un mensaje en el muro a su fundador "Lo siento por invadir su privacidad. "No tuve otra alternativa después de todos los informes que envié al equipo de Facebook... Como puede ver no estoy en su lista de amistades y de todos modos puedo colocar comentarios"
Leer más en: http://www.elmundo.com.ve/noticias/tecnologia/programas/-hackean--cuenta-de-facebook-de-mark-zuckerberg.aspx#ixzz2cqcjYzFC

[11] Noticia disponible en: http://www.elmundo.es/america/2012/10/17/noticias/1350498777.html

[12] Disponible en: http://www.prnewswire.com/news-releases/whos-watching-you-data-privacy-day-survey-reveals-your-fears-online-114793269.html

La sociedad ha confiado en las nuevas tecnologías para mejorar la educación pero ha fallado en incorporar de forma sistemática la cultura de la seguridad en internet, además de comportamientos éticos y responsables, por lo que un mayor número de jóvenes y adultos se han convertido en víctimas y autores de delitos permitidos por el abuso de la tecnología como la deshonestidad académica (violación a los derechos de autor), la piratería de música y videos, acoso y amenazas y fraudes, entre otros (Mcquade, 2007). No sería descabellado pensar que el cibercrimen ataca más personas que empresas[13], ya que la falta de cultura de cómo protegerse en la red[14] y de los riesgos potenciales que impone el no hacerlo, limita la responsabilidad que puedan tener los individuos al usarla, convirtiéndolos en *ciberincautos*[15] y potenciales víctimas

Sukhai (2004) menciona que términos como ciberciudadanía, ética cibernética y netiqueta, reflejan un comportamiento socialmente responsable en el ciberespacio, relacionado a lo que las personas hacen bajo el anonimato que ofrece la red. Dicho comportamiento se hace necesario, no solo como una protección contra el cibercrimen, sino para proteger el ciberespacio de los usos abusivos del mismo por parte de sus usuarios.

¿CUÁL HA SIDO LA RESPUESTA DE LA COMUNIDAD MUNDIAL?

El 23 de noviembre de 2001 la Unión Europea junto con Estados Unidos, Canadá, Japón y Sudáfrica, firmaron el Convenio de Budapest[16], cuyo objetivo es intensificar la cooperación entre los Estados firmantes[17] en la lucha contra la cibercriminalidad y en la protección de los intereses vinculados a las TIC's a favor de ofrecer respuestas eficaces, rápidas y coordinadas en la detección, investigación y persecución de estos delitos. Para ello, se comprometieron a adoptar medidas necesarias para prever como infracción penal a todas aquellas acciones que atentan contra la propiedad intelectual, la intimidad, el contenido, el acceso no autorizado y el sabotaje. Adicionalmente, definieron el derecho procesal, las condiciones y garantías, así como los lineamientos de cooperación internacional que regirán su acción.

Salom (2005) indica que en esta Convención se agruparon los delitos informáticos en cuatro grupos:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso e interpretación ilícita así como la interferencia de datos).

- Delitos por su contenido tales como la pornografía infantil y xenofobia.

- Delitos relacionados con la informática como la falsificación y fraude.

- Delitos relacionados con las infracciones a los derechos de propiedad.

La Unión Europea ha sido quien ha liderado estas acciones, no solo por la firma y promoción del Convenio de Budapest, sino por sus propuestas institucionales:

- En el 2009 propuso la creación de un tribunal de delitos informáticos, que en un principio atendería los delitos de fraudes telemáticos, usurpación de identidades y otras variantes. No se dieron detalles de la jurisdicción que tendrá, pero sí destacó la necesidad de imponer límites definidos al intercambio de información entre los Estados miembros y al uso de registros comunes de la UE.

[13] StrategyOne (2010) afirma que el 65% de los usuarios de internet han sido víctimas del cibercrimen.
[14] Norton Cybercrime Index permite a los usuarios conocer cuál es el nivel de riesgo que enfrenta al conectarse a internet, ofreciéndoles un análisis gráfico y estadístico del mismo. Este índice fue desarrollado por la empresa Symantec como un software de soluciones de seguridad.
[15] StrategyOne (2010) afirma que uno de cada 10 se culpan a sí mismos por haber sido víctima del cibercrimen.
[16] Balanta (2009) considera que es necesario actualizar el convenio ya que no contempla el phishing, la suplantación de identidad, entre otros delitos.
[17] Para el 2011 no todos los países habían ratificado el Convenio, tal es el caso de Reino Unido. Salom (2005) indica que Albania lo ratifico el (20-06-02), Croacia (17-10-02), Estonia (15-05-03), Hungría (04-12-03), Lituania (02-03-04) y Rumania (12-05-04).

- En Noviembre de 2010, la UE, EEUU y la OTAN acordaron desarrollar tres sistemas con el objetivo de aumentar la seguridad que iniciarán sus labores el 2013: un Centro dedicado a la defensa ante el cibercrimen, un Sistema de Alerta e Intercambio de Información Comunitario "EISAS" sobre delitos informáticos y una Red de Equipos de Respuesta Informática Urgente. La OTAN por su parte, aprobó el capítulo Strategic Concept que incluye planes para desarrollar nuevas capacidades contra ciber ataques a instituciones militares.

Gamba (2010), sostiene que si bien existen delitos que ya son tratados internacionalmente, la experiencia en la Unión Europea indica que la modificación de la normativa no ha sido suficiente, pues se requieren medidas no legislativas como la creación de unidades nacionales especializadas que cuenten con capacitación permanente. Dichas medidas enfrentan un límite fundamental en la disponibilidad de recursos, lo que define su real capacidad de frenar este tipo de actividades, aún contando con normativa específica que lo facilite.

Por ejemplo, América Latina, destina cerca de 400 USD per cápita anual al desarrollo de las TIC's y los países desarrollados gastan entre 2.000 y 3.000 USD anuales. Esta brecha y las diferentes realidades, definen una importante restricción de recursos para la región ya que limita su capacidad de adaptarse a los estándares propuestos por los países desarrollados.

Gamba (2010), también resalta la importancia y la necesidad de establecer redes de confianza entre las agencias nacionales, con el fin de crear una red de investigación y punición que no se obstaculice con las fronteras, ya que este tipo de delitos tienen implicaciones en la seguridad nacional y en labores de inteligencia, lo que tiende a disminuir la colaboración entre países. Chung et al. (2004) recomiendan actualizar las leyes existentes, mejorar y ampliar las tareas de los equipos especializados, utilizar recursos cívicos (investigadores de universidades) para obtener soporte técnico, promocionar las investigaciones de los delitos cibernéticos y realizar estudios de las medidas ejecutadas por los países para identificar buenas prácticas.

Lo anterior se complementa con el fomento y desarrollo de las iniciativas privadas, como la Black Hat Conference que durante 15 años ha ofrecido un espacio para compartir investigaciones de alto nivel sobre seguridad, en donde revelan las vulnerabilidades de los sistemas y sus impactos tanto para consumidores como a las infraestructuras de servicios a nivel internacional. También merece mención la WhiteHat[18] Security, empresa dedicada a proveer seguridad web en una amplia escala y precisión, que también realiza sesiones anuales de ejecutivos dónde discuten y plantean diferentes soluciones a las vulnerabilidades que identifican en la red. Ambas son ejemplos de lo valioso que resulta congregar a las "mentes" de la industria en pro de desarrollar medidas que incrementen la seguridad y el "buen uso" de la web. Sin embargo, la cobertura y difusión de estas actividades no excede la de revistas especializadas en la materia.

¿CUÁL HA SIDO LA RESPUESTA DE AMÉRICA LATINA?

La Declaración de Georgetown en el 2001, evidencia la prioridad que le ha dado América Latina a generar propuestas regulatorias que den cuenta de la convergencia tecnológica y de negocios a favor de ofrecer condiciones que abaraten los costos, incentiven y aseguren la continuidad de las inversiones.

La discusión se ha focalizado en cómo se desarrolla una sociedad de información que promueva el desarrollo y la equidad. Por lo que la respuesta de la región en la materia se puede considerar reactiva ya que se ha enfocado principalmente en la penalización del uso de las TIC's en temas sensibles como la pornografía infantil, en el desarrollo de peritaje forense y en la creación de brigadas digitales o cuerpos especializados para enfrentar estos crímenes. Sin

[18] WhiteHat es un término que se le atribuye a los hacker que usan sus habilidades informaticas por el bien común, ya que encuentra, alerta y en algunos casos soluciona vulnerabilidades en la red antes de que los "hacker malos" las identifiquen y causen daño con ello.

embargo, no cuenta con una cantidad de leyes suficientes que le permita afrontar las diferentes tipologías de crímenes y su carácter transnacional, con la capacitación suficiente del sistema judicial, ni con normativas armonizadas.[19]

Las respuestas ofrecidas por los países de la región se han orientado principalmente a modificar la ley penal (Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay y Perú), seguido por la introducción de leyes específicas (como el caso de Brasil, Chile, Colombia y Venezuela). Ecuador, por su parte, ha usado una ley civil y comercial para introducir sanciones penales, mientras que Uruguay solo prevé una ley de Protección a los Derechos de Autor. En los países en que no ha habido aún una reforma en este campo, se trata de "reinterpretar" la normativa vigente en materia penal para incluir la tipología de delitos informáticos (Gamba, 2010).

Los grupos subregionales, como la Comunidad Andina (CAN), el Mercosur, Centro América y el Caribe han emprendido esfuerzos por crear normas armonizadas. La CAN ha avanzado en la firma digital y en la contratación electrónica, el Mercosur en temas de protección a la privacidad, mientras que Centro América y el Caribe aprovecha las ventajas de la experiencia acumulada, evitando los errores de otros países en la revisión de sus legislaciones (Cepal & EuroAid, 2005).

Estas acciones también obedecen al cumplimiento del compromiso adquirido en la Declaración de Florianápolis en el 2001, donde los países de la región acordaron promover la creación de un observatorio regional para monitorear el impacto de las TIC's sobre la economía, lo que requiere el fomento de políticas que armonicen normas y estándares a favor de crear marcos normativos que brinden confianza y seguridad a nivel nacional y regional, tal como lo señala La Meta 25 del Plan de Acción sobre la Sociedad de Información de América Latina y el Caribe, eLAC 2007.

Pese a los esfuerzos a nivel subregional, las diferencias en las condiciones incipientes de cada subregión son un obstáculo a la armonización y una oportunidad que ofrece espacios abiertos para el diseño e implementación de respuestas estructurales adaptadas a la realidad presupuestaria, institucional y tecnológica de la región. La Meta 25 del Plan de Acción sobre la Sociedad de Información de América Latina y el Caribe, eLAC 2007 considera que es más sencillo iniciar el proceso de armonización a nivel subregional, ya que contaría con una normativa legal que les sirva como esquema para integrarse con otras subregiones de una forma más eficiente.

A la fecha, hay muchas tareas pendientes tales como solucionar confusiones terminológicas; el desarrollo de propuestas regionales que permita la interacción de actores jurídicos que respeten la legislación y jurisdicción de cada país; ofrecer capacitación al poder judicial y a la policía de investigación en estos temas; la creación de agencias nacionales que sean coordinadas regionalmente; crear mecanismos de resolución de disputas en transacciones electrónicas; definir fuentes de financiamiento, entre otros. La necesidad de resolver las tareas pendientes se acrecienta con las siguientes cifras de la 15º edición del Internet Security Threat Report (2009) de Symantec: (Fernández de Lara, 2010)[20] Brasil generara el 6% de toda la actividad maliciosa en la web, ubicándose en el tercer lugar del ranking mundial. (ii) El ranking de generación de actividad maliciosa en AL: México y Argentina (13%), segundo y tercer lugar, seguidos por Chile que genera el 7%. (iii) Países de Origen de los ataques cibernéticos hacia América Latina: Estados Unidos 40%, Brasil 13% y México 5%. (iv) México ocupa el lugar 16 en el mundo, como país origen de ataques, representado el 1% de los mismos. (v) 14% de los computadores zombis del mundo, se encuentra en la región. Brasil alberga al 7% de éstos. (vi) América Latina generó 20% de todo el spam en 2009: Brasil 59%, seguido de Colombia y Argentina con el 12%.

Iriarte (2005) menciona que los esfuerzos normativos que se han realizado en la región evidencian voluntad política para desarrollar sistemas jurídicos que respondan a los cambios tecnológicos de las TIC's, pero destaca que muchas veces responden a una fundamental falta de visión y entendimiento de las tecnologías que se intenta regular, lo que explica por

[19] Se han presentados intenciones aisladas en las que se han planteado evaluar el adherirse al Convenio de Budapest, tal ha sido el caso de Argentina, Ecuador, Chile y México.
[20] Noticia Disponible en: http://www.netmedia.info/ultimas-noticias/el-rostro-del-cibercrimen-en-al/
El Informe: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

qué tienden a no cumplir con su objetivo. Asimismo, enfatiza en la importancia de pensar en forma estructural al momento de desarrollar e implementar nuevas formas regulatorias a favor de que se adapten a los retos que impone la sociedad moderna y sus realidades, sin que se limiten a copiar soluciones de otros países. De suceder lo contrario, se presencian situaciones reactivas como la de Brasil, en donde el escándalo y conmoción que causó la violación de la privacidad (fotos y otros datos personales) y extorsión a la actriz Carolina Dieckmann, sirvió de "detonante y/o estímulo" para que los legisladores tomaran cartas en el asunto y formularan la "Ley Carolina Dieckman" y la Reforma al Código penal (que tipifica estos delitos y los sanciona con cárcel) y cuya aplicación se inició en el 2013.

- **LA LUCHA CONTRA EL CIBERCRIMEN *¿UN RETROCESO EN LOS DERECHOS INDIVIDUALES?***

Rubio (s/f) afirma que el control de la información ha constituido la base del poder del Estado a lo largo de la historia. Indica que el carácter descentralizado de la Red permite la creación de innumerables medidas de control, pues los métodos para censurarla son variados y van desde la prohibición a su acceso (como ha ocurrido en Afganistán y Corea del Norte), el control restrictivo del acceso por medio de autorizaciones exclusivas (Cuba), la monitorización por medio de una brigada policial (China), el uso de filtros de contenido y bloqueo de sitios (Arabia Saudí), la creación ISP que pertenecen al Estado y el uso de redes de espionaje como Echelon o Carnivore o casos extremos como el desconectar al 80% del país por ataques de hackers durante un día electoral (Venezuela). Sin considerar las medidas legales como USA Patriot Act de EEUU que legalizó en el 2001 la vigilancia de internet permitiendo al FBI fiscalizar mensajes electrónicos así como la creación de servidores centrales para "pinchar" los equipos sospechosos. Esta acción, ha sido motivo de gran polémica recientemente a raíz de las revelaciones de Edward Snowden ex técnico de la CIA a los diarios The Guardian y The Washington Post, en las que indicó que la Agencia de Seguridad Nacional[21] a través del programa de vigilancia electrónica PRISM recopilaba información privada de los principales servidores y presionaba a empresas de telecomunicaciones para que entregaran los registros de las actividades telefónicas de sus clientes. Además de ello, fue revelado el hecho de que EEUU a través del programa XKeyscore se puede buscar y guardar lo que cualquier usuario hace en internet (correos, redes sociales, entre otros) sin ningún tipo de autorización.[22]

Es por ello que este auge de crear medidas que enfrenten el cibercrimen o que otorgan poderes especiales a los gobiernos justificadas en la protección de los intereses de la Nación ha encontrado resistencias en diferentes sectores de la sociedad y entre países también, las cuales se han avivado en los meses recientes debido a las revelaciones de Snowden:

- Center of Democracy and Technology, entre otras asociaciones de ciberderechos, temen que este tipo de convenios[23] de vía libre a la invasión de la privacidad de los usuarios y al consiguiente control (o represión) gubernamental por lo que enfatizan en la importancia de que dichas regulaciones respeten y garanticen los derechos humanos y las libertades fundamentales, tal como lo expresaron en Túnez 2005.
- Los proveedores de internet representados por Internet Content Rating Association han iniciado autorregulaciones que tratan de minimizar la interferencia del Estado, como una alternativa a lo que califican como una censura legislativa.
- Enrique Gimbernat (2004)[24] afirma que los derechos humanos y su antítesis, los delitos, son los mismos fuera y dentro de la Red. Que si bien pueden establecerse tipologías de delito, serán clasificaciones inútiles que siempre estarán condicionadas a la evolución de la técnica. Adicionalmente, destaca que estas regulaciones están criminalizando una serie de actos cotidianos que solo favorecen a empresas vinculadas al sector de

[21] The Wall Streat Journal indica que la NSA (por sus siglas en ingles puede espiar el 75% del tráfico de internet en EEUU.
[22] Disponible en: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
[23] Ej. Convenio de Budapest.
[24] Entrevista disponible en: http://www.noticiasdot.com/publicaciones/2004/0604/1606/noticias1606004/noticias160604-3.htm

telecomunicaciones que amparadas por la ley consiguen consolidar beneficios económicos, sin que la ley consiga ofrecer seguridad jurídica alguna al medio informativo. Gimberlat enfatiza en la necesidad de redefinir la escala de valores que se maneja a favor de atribuir penas coherentes con la falta cometida y que garantice el respeto y protección de los derechos de particulares, así como lo hacen con los derechos de las empresas.

- Los organismos europeos de protección de datos han manifestado la necesidad de revisar de forma más precisa las legislaciones nacionales sobre la vigilancia de los ciudadanos. A su vez, piden que se aclare de forma exacta el tipo de informaciones que ha captado EEUU (caso PRISM) y las acciones a las que pueden recurrir los ciudadanos europeos cosa de evaluar si las acciones de EEUU han estado al margen o no del derecho internacional. También piden averiguar la existencia de programas similares en la Unión Europea.[25]
- En la región, ha sido Brasil el país que ha reaccionado con mayor rapidez pues ha considerado implementar políticas que obliguen a las empresas internacionales de internet a almacenar los datos en Brasil y no en el exterior. Además, estudia la posibilidad de formalizar un pedido a la ONU para que mejore la seguridad cibernética internacional, de manera de evitar que sus ciudadanos y sus empresas sean espiadas por países extranjeros (tal fue el caso de EEUU).

A pesar de estas reacciones y lo válido de sus argumentos, la participación y el liderazgo del Estado es necesaria e importante ya que no solo debe proteger la integridad de sus ciudadanos creando mecanismos que desincentiven las actividades delictivas ejecutadas tanto por particulares u organizaciones criminales, sino también de las empresas de telecomunicaciones, que son las encargadas de proveer el acceso y desarrollar software para sus múltiples usos. Un ejemplo de esto es la reciente multa de 100.000 euros que le aplico la Comisión Nacional de la Informática y las Libertades francesa a Google por recolectar datos personales con los carros Street View.

Por último, destaca la vulnerabilidad de los software. Kannan y Telang (2005) sostienen que se ha convertido en un área crítica para los hacedores de política, ya que el incremento de las vulnerabilidades ha creado un mercado que las identifica y las comercializa como información a las firmas interesadas para que se protejan[26], lo que abre la interrogante de qué es preferible: si permitir un monopolio o que el estado provea este servicio como un bien público. En dicho estudio se argumenta que permitir un monopolio reduce el beneficio social ya que el monopolista siempre tendrá incentivos a permitir fugas de cualquier vulnerabilidad que identifiquen a favor de obtener mayores clientes en un futuro, por lo que indican que el mejor mecanismo es permitir que funcionen instituciones como Computer Emergency Response Team (CERT). Adicionalmente, proponen idear un modelo de cooperación entre la CERT y empresas privadas para identificar el efecto en el bienestar, aunque no están seguros de su factibilidad empírica.

Everett (2009) destaca que debe existir una responsabilidad compartida entre los individuos y las comunidades, a favor de que colaboren con las instituciones policiales a fiscalizar internet y de crear círculos virtuosos que complementen y agilicen las labores de las agencias encargadas de cumplir las nuevas disposiciones legales que han surgido como respuesta al cibercrimen.

CONCLUSIONES Y RECOMENDACIONES DE POLÍTICAS PÚBLICAS

El desafío que imponen las TIC's de crear nuevas reglas de convivencia en la red que tengan un carácter transnacional es ineludible. El impacto que tendrán estas regulaciones dependerá de la conjugación de realidades como la capacidad institucional, estructura de sus mercados, el desarrollo tecnológico y la cultura de sus ciudadanos, por lo que no es muy factible esperar resultados homogéneos.

[25] DIsponible en: http://tecno.americaeconomia.com/noticias/autoridades-europeas-de-proteccion-de-datos-investigan-el-programa-prism
[26] Inicialmente Computer Emergency Response Team (CERT) reportaban voluntariamente las vulnerabilidades que encontraban. Posteriormente surgió una firma IDefense que vende dicho servicio.

Si bien las diferencias estructurales de la región condicionan la capacidad de implementar sistemas uniformes de forma eficiente, no implica que no sea viable desarrollar legislaciones armonizadas y con carácter cooperativo entre naciones que respondan a sus realidades y capacidades. Pero para ello es necesario que los Estados latinoamericanos sean los autores y actores de su rol en el ciberespacio. A pesar de ello, América Latina tiene las siguientes opciones:

1. Mantener una postura pasiva: no hacer nada y que cada país continúe avanzando de forma independiente en materia legislativa, comprometiéndose o no con las iniciativas expuestas.

A pesar de que esta discusión no es una prioridad explícita, representa una urgencia latente (e ignorada) que debe ser considerada en la agenda, por lo que se debe aprovechar la ventana de oportunidad que el caso Snowden ha abierto para el desarrollo de este debate.

Si bien el continuar "ignorando" esta realidad permitiría aprovechar algún beneficio implícito de no contar con un sistema legal armonizado (ej. evadir derechos de autor), la principal desventaja radica en que América Latina puede suscribir de forma rápida y arbitraria este tipo normas, adquiriendo compromisos que le imponga nuevas restricciones a su desarrollo.

2. Adoptar una postura proactiva: esta opción abarcaría dos ámbitos principales: el debate interno a nivel de país y otro a nivel internacional orientado a impulsar y promover el proceso de armonización de las regulaciones en la región.

Esto requiere tener una visión de la situación actual y sus retos a favor de consolidar un liderazgo que exprese una *dirección* (qué se quiere lograr), *protección* (estaremos mejor, esto es necesario para todos) y *orden* (cómo se hará). El costo de esta alternativa es el intenso lobby que se debe desarrollar a diferentes instancias. Si se adopta esta postura, se recomienda una *política* que haga énfasis en lograr *un consenso técnico* e identificar (o crear) una *fuente de financiamiento* como *condiciones necesarias* para iniciar el proceso de armonización; a favor separar el tema del *cómo* y *con qué* de la discusión. Para esto se requiere:

- Convocar un equipo multidisciplinario[27] integrado por representantes de los gobiernos, sector privado (usuarios y proveedores), organizaciones civiles y organismos internacionales para conocer los avances de la región en materia de infraestructura e identificar potencialidades y limitantes en la creación de instituciones similares a las propuestas por la Unión Europea. Todo, con la finalidad de identificar la opción técnica más viable para la región.

  Tal como se mencionó en el desarrollo de este documento, la promoción de espacios técnicos que permitan a los diferentes actores interactuar e intercambiar experiencias y opiniones es, además de un activo invaluable como fuente de alternativas, una necesidad para el diseño de las políticas públicas en la materia, por las requerimientos técnicos que implican.

- Impulsar la creación de un *fondo* para obtener recursos que financien la plataforma y el funcionamiento institucional del ente encargado de diseñar, implementar y ejecutar el nuevo sistema armonizado, ya que es importante tener presente que los acuerdos suscritos serían letra muerta si la región no tiene los medios financieros para crear las capacidades técnicas y estructuras institucionales que le den vida.

Resuelto esto, se plantea establecer un *Comité* que diseñe la creación de una *Agencia Multilateral* (en adelante AM) que se encargue de desarrollar las siguientes acciones:

-Revisión y Armonización de las legislaciones.

-Creación de Brigadas policiales contra el cibercrimen.

[27] Hilbert, Miles y Othmer (2009) sostienen que las lecciones aprendidas de eLAC Policy Priorities Delphi incentivaron la participación, transparencia y rendición de cuentas en las decisiones de políticas públicas.

-Creación de Tribunales de justicia para las TIC's.

-Creación de centros de capacitación y desarrollo. (Información especializada).

-Creación de campañas informativas y preventivas para público general.

-Diseño de normativa para la colaboración internacional.

-Definición de un mecanismo de arbitraje internacional.

-Promoción del sistema y funcionamiento creado.

El desarrollo de estas áreas permitirá contar con legislación, medios de investigación y persecución, justicia y capacitación para ofrecer respuesta a los delitos con y en las TIC's.

Esta política ofrece la oportunidad de crear un diseño institucional para América Latina fundado en espacios de diálogo y consenso ya que no solo existe la necesidad de legislar y prevenir sino de respetar los derechos y las libertades de las personas, por lo que es necesario llegar a un acuerdo o pacto social y regional que de sostenibilidad y viabilidad al nuevo sistema legal en la materia. Sin embargo, enfrenta su mayor dificultad en identificar el grado de autonomía (o dependencia) que tendrán las agencias nacionales (entendiéndose como pequeñas sedes) del Poder Judicial y del Ministerio de Defensa de cada país con respecto a la Agencia Multilateral, pues no se puede olvidar las implicaciones que tienen en la Seguridad Nacional y los conflictos de interés que genera, tal como lo hemos presenciado en los últimos meses.

Independientemente de cuál sea la opción que se seleccione, los Estados que integran la región deberían buscar financiamiento para diseñar y promover una cultura del buen uso de la red, donde los ciudadanos adquieran conciencia de que los riesgos son reales y que es necesario aprender a reducirlos o evitarlos, pues la mejor respuesta para luchar contra el cibercrimen es la prevención, y ésta se obtiene educando e incentivando a los ciudadanos a involucrarse activamente en el compromiso de salvaguardarse en la red.

BIBLIOGRAFÍA

Ponencias

Baker, Wade H.; Hylender, C.David; Valentine, J.Andrew. 2008 Data Breach Investigations Report. Verizon Business RISK Team. Disponible en: http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Balanta, Heidy. (2009). **Aproximación legal a los delitos informáticos una visión de derecho comparado.** Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal.

Convenio sobre la ciberdelincuencia. Budapest, 23.XI.2001. Council of Europe. Serie de Tratados Europeos No. 185. Disponible en: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

Informes

Informe sobre el Cibercrimen 2008. S21sec. 2008. Disponible en: http://www.s21sec.com/descargas/S21sec-ecrime-Informe-Cibercrimen-2008.pdf

Maliciuos Software (Malware): A Security Threat to the Internet Economy. (2007). Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL. The Organisation for Economic Co-operation and Development (OECD). Disponible en: http://www.oecd.org/dataoecd/53/34/40724457.pdf

Symantec Global Internet Security Threat Report Trends for 2009. Symantec. Volume XV, Published April 2010. Disponible en: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

Norton Cybercrimen Report: The Human Impact 2010. Norton by Symantec. Disponible en: http://us.norton.com/theme.jsp?themeid=cybercrime_report

Documentos Electrónicos:

Rubio Moraga, Ángel L. (s/f). **Censura en La Red: Restricciones a La Libertad de expresión En Internet**. Universidad SEK de Segovia. Disponible en: http://www.ucm.es/info/hcs/angel/articulos/censuraeninternet.pdf

Mcquade, Samuel. (2007). **We Must Educate Young People About Cybercrime Before They Start College.** The Chronicle of Higher Education**.** Information Technology Volume 53, Issue 14, Page B29. Disponible en: http://chronicle.com/article/We-Must-Educate-Young-People/23514

Governing the InternetSource: Economic and Political Weekly, Vol. 40, No. 46 (Nov. 12-18, 2005), pp. 4789-4792. Published by: Economic and Political WeeklyStable URL: http://www.jstor.org/stable/4417381

Papers Publicados

Brenner, Susan W; Koops, Bert-Jaap. (2004).**Approaches to Cybercrime Jurisdiction.** Journal of High Technology Law. Vol. IV No. 1. ISSN 1536-7983.

Cárdenas Aravena, Claudia. (2008). **El lugar de comisión de los denominados ciberdelitos**. *Polít. crim.*, N° 6, 2008, A2-6, pp. 1-14.

Chawki M. (2005). **A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy**. DROIT-TIC, 11 avril 2005

Chung, Wingyan; Chenb, Hsinchun; Changc, Weiping and Chouc, Shihchieh. (2004). **Fighting cybercrime: a review and**

Everett, Catherine. (2009). **Who is responsible for policing the internet?.** Computer Fraud & Security. May 2009.

Fernández Teruelo, Javier Gustavo. (2007). **Respuesta Penal Frente a Fraudes Cometidos En Internet: Estafa, Estafa Informática y Los Nudos de La Red.** REVISTA DE DERECHO PENAL Y CRIMINOLOGÍA, 2.a Época, n.o 19 (2007), págs. 217 -243.

Gamba, Jacopo. (2010). **Panorama del derecho informático en América Latina y el Caribe.** Colección de Documentos y Proyectos 39. Cepal. Disponible en: http://www.eclac.org/ddpe/publicaciones/xml/8/38898/W302.pdf

Hilbert, Martin; Miles, Ian; Othmer, Julia. (2009). **Foresight tools for participative policy-making in inter-governmental processes in developing countries: Lessons learned from the eLAC Policy Priorities Delphi**. Technological Forecasting & Social Change 76 (2009) 880–896.

Iriarte Ahon, Erick. (2005). **Estado situacional y perspectivas del derecho informático en América Latina y el Caribe.** Cepal y EuropeAid. Disponible en: http://www.eclac.org/publicaciones/DesarrolloProductivo/5/LCW25/LCW25.pdf

Kannan, Karthik; Telang, Rahul. (2005). **Market for Software Vulnerabilities? Think Again.** Management Science Vol. 51, No. 5, May 2005, pp. 726-740 DOI: 10.1287/mnsc.1040.0357.

Kleve, Pieter; De Mulder, Richard; van Noortwijk, Kees. (2011). **The definition of ICT Crime**. Computer Law & Security review 27 (2011) 162-167.

Salom C., Juan (2005). **La investigación del Delito Informático en la Guardia Civil.** Colección "Estudios de Derecho Judicial" – CGPJ, 71-2005.

Speer, David l.(2000). **Redefining borders: The challenges of cybercrime.** Crime, Law & Social Change 34: 259–273, 2000.

Sukhai, Nataliya B.(2004). **Hacking and Cybercrime.** InfoSecCD Conference'04, October 8, 2004, Kennesaw, GA, USA. Copyrigh 2005.

Parker, D.B.(1998).**Fighting Computer Crime: A New Framework for Protecting Information**. Wiley Computer Publishing, Chichester, England, 1998.

Philippsohn, S.(2001).**Trends in cybercrime an overview of current financial crimes on the internet.** Computers & Security 20 (1) (2001) 53–69.

Power, R. (2002). **CSI/FBI computer crime and security survey**. Computer Security Issues & Trends 8 (1) (2002) 1 –22.

Reidenberg, Joel R.(2005).**Technology and Internet Jurisdiction**. University Of Pennsylvania Law Review. Vol. 153: 1951.

Web Side:

Center of Democracy and Technology: http://www.cdt.org/

Computer Emergency Response Team (CERT): http://www.cert.org/

Internet Content Rating Association: http://www.fosi.org/icra/

Kaspersky Lab: http://www.kaspersky.com/sp/news

The Comprehensive National Cybersecurity Initiative: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe (OSILAC) http://www.eclac.org/socinfo/osilac/