www.flacsoandes.edu.ec

44

2011

Ciudad Segura

PROGRAMA ESTUDIOS DE LA CIUDAD FLACSO - ECUADOR

DELITOS INFORMÁTICOS

El hábil delincuente

Jaime Erazo Espinosa

Hace tiempos ya, un muy pensado enredo entre sistemas y aparatos informáticos y de comunicación con un específico conjunto de actividades estatales, de gobierno, de mercado y sociedad, iniciaron un espacio y mundo nuevo y virtual que hoy lo conocemos como cibernético y digital; a partir de su origen, se aceleró el desplazamiento y la interacción de no tan sólo lo material puntual sino de lo general, progresando también y por un lado, la institucionalización cada vez más sofisticada de nuevos ambientes imaginados, y por otro, la caracterización global de sus efectos como son la inmediatez y la imposibilidad de enfoques exactos. El nuevo y virtual espacio y mundo es acelerado, su velocidad desestabiliza órdenes establecidos y crea, entre variadas formas, u oportunidades tan simples o tan complejas como el "email" o Facebook, o comportamientos tan perturbadores como los violentos.

Ante él hay un espectro de inquietudes e incapacidades públicas, privadas e individuales: unas con respecto a su desarrollo, otras con respecto a su uso y ambas con respecto a su gobernanza. Las primeras tienen correlación con los sistemas educativos e investigativos que en países como Bolivia, Ecuador, Honduras, Nicaragua, Paraguay y Venezuela, son pobres; las segundas con la estructura jurídica, nacional y compartida a nivel internacional, de principios, normas, reglamentos y procedimientos de control y regulación; y las terceras con los marcos políticos que dictaminan las prioridades y las eficiencias de sus, por ejemplo, programas tanto de acceso universal como de competitividad.

Dentro del ciberespacio/mundo digital, su tecnología constitutiva complejiza y problematiza la seguridad, facilita el cometimiento de delitos, dificulta la prevención, detección y procesamiento de los mismos y, por tener alcance global, la persecución de los mentores/hacedores de ilícitos informáticos se asemeja a sus mismos ataques, es decir, a procesos sin discreción alguna. Así, la violencia dentro de lo virtual ha aumentado de nivel y se ha generado, sin limites, en cualquier parte del mundo convencional; sus condiciones, mecanismos y estrategias se comparten y protegen con el anonimato de quienes las generan. Y es que estos ciber y hábiles delincuentes, generadores de delitos informáticos, actúan violentando la información primada y privada de cualquiera (identidades, contraseñas, números de tarjetas y cuentas) para luego usarla en la confección de ilícitos concretos, entre los cuales tenemos: accesos, desvíos y apoderamientos ilegales (ej.: *wa r dialing*); fraudes, daños y sabotajes financieros (ej.: *phishing* o *pharming*); acosos y abusos a infantes y adolescentes (ej.: *sexting, grooming* o *bullying*); ataques a infraestructuras de gobiernos y organizaciones (ej.: *hacking*); extorsiones y suplantaciones (ej.: *spoofing*); etc. Un ilícito virtual involucra siempre sistemas y aparatos informáticos o de comunicación: la Internet es la red electrónica que por su estructura tecnológica más ha permitido acoger a quebrantadores de la privacidad individual, junto a ella, la piratería ha producido millones de dólares en pérdidas en países tan dispares como México y Paraguay, el primero ocupó en 2009, el dieciseisavo lugar en tasa de piratería en América Latina (59%) y el segundo en pérdidas dentro de la misma región ($823 millones); por el contrario, el segundo en el mismo año, ocupó el segundo lugar en tasa (83%) y el dieciseisavo en pérdidas ($16 millones). Tanto la irrupción en la seguridad personal como el robo de derechos de autor ya están tipificados como delitos en los marcos jurídicos de nuestros países, cuando ellos son realizados en el ciberespacio/mundo digital, se los considera como variaciones de tipo y su penalización depende, primero de que haya norma y segundo, del mayor o menor rol de la tecnología en el incurrimiento del crimen electrónico.

Lo virtual y sus canales, ni son confiables ni son honestos, y aunque por derecho constitucional o leyes orgánicas –como la de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador, 2002) o la 26.388 de Delitos Informáticos (Argentina, 2008)–, todo ciudadano tiene el privilegio de proteger sus datos personales cuando usa sistemas o aparatos informáticos o de comunicación, las infraestructuras digitales de nuestros países no son seguras (con rigurosos estándares) y no son privadas (exceptuando las intervenciones públicas de inteligencia). Por el contrario, las precauciones de los usuarios primero y después las de los desarrolladores, son medidas espontáneas que pretenden, sin sacrificar la privacidad, garantizar una segura convivencia ciudadana en el ciberespacio

Libros

Nava Garcés, Alberto (2005).
Análisis de los delitos informáticos.
México: Editorial Porrúa. ISBN: 970-07-5605-X.
119 páginas.

Este trabajo acomete el tema de los delitos informáticos, los cuales son expuestos como variaciones de delitos ya tipificados, con la característica de ser realizados con computadoras. Para ello, se explica en primer término el mundo de la informática dentro del derecho. Posteriormente, se estudian los delitos informáticos en particular, destacando los rasgos que interesan a la dogmática penal y brindando un amplio panorama sobre la materia, porque, además de la legislación aplicable, se complementa con la referencia de jurisprudencia, tesis relacionadas y publicaciones periódicas.

Littlejohn Shinder, Debra (2003).
Prevención y detección de delitos informáticos. Ed. Anaya Multimedia. ISBN: 844151545X. ISBN-13: 9788441515451. 832 páginas.

Esta obra proporciona una amplia visión del ciber-crimen: lo que es y lo que no es, sus diferencias y similitudes con otros tipos de crimen y cómo se puede separar el amplio concepto de "ciber-crimen" en varias categorías que faciliten su discurso, legislación, persecución e, idealmente, prevención. El libro revisa el arte y la ciencia de los perfiles criminalísticos, así como el modo de proceder cuando uno se ha convertido en víctima de tales ataques. También se tratan otros aspectos indispensables para comprender esta problemática, entre ellos los conceptos de la seguridad informática y de redes, las intrusiones y los ataques en la red, las funciones del *hardware* de las redes (*hubs*, *switches*, *routers* y demás), además de la importancia del software del cliente y el servidor, los sistemas de archivo de las redes y los protocolos. Identifica los pasos que se pueden dar para proporcionar las conexiones de banda ancha, las formas de asegurar su explorador *web* y los mecanismos con los cuales los administradores de redes pueden proteger a sus servidores de los ataques.

Páginas web

Business Software Alliance (s/f).
Visita 14 de septiembre en http://www.bsa.org/country.aspx?sc_lang=es-AR

"Delitos Informáticos" (s/f).
Visita 14 de septiembre de 2010 en http://www.delitosinformaticos.com/

"Monitor de privacidad y acceso a la información en América Latina" (s/f).
Visita 14 de septiembre de 2010 en http://www.alfa-redi.com/privacidad/

Recovery Labs (s/f). "Servicio integral de peritaje informático".
Visita 14 de septiembre en http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Enlaces on line

Arias Chaves, Michael (2006). **"Panorama general de la informática forense y de los delitos informáticos en Costa Rica".** En *Revista de las sedes regionales* Vol. VII N.° 12. Universidad de Costa Rica: InterSedes.
Disponible en http://redalyc.uaemex.mx/redalyc/pdf/666/66612867010.pdf

Gamba, Jacopo (2010). **Programa del derecho informático en América Latina y el Caribe** Chile: Comisión Económica para América Latina y el Caribe (CEPAL).
Disponible en
http://www.eclac.cl/ddpe/publicaciones/xml/8/38898/W302.pdf

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

Mendoza, Eugenio y Eugenio Urdaneta (2005). **"La telemática y los delitos informáticos en Venezuela".** En *Telematique* Vol. 4 N.° 001. Universidad Rafale Belloso Chacin de Venezuela.
Disponible en http://redalyc.uaemex.mx/pdf/784/78440106.pdf

POLÍTICA PÚBLICA

El control del ciberespacio

Alfredo Santillán

Sin duda, uno de los mayores retos del presente siglo es lograr un buen nivel de seguridad en el ciberespacio. En vista del incremento cuantitativo y cualitativo del uso de las TIC en todas las actividades sociales, éstas han dejado de ser instrumentos opcionales en la vida cotidiana y han llegado a ser vitales en la medida en que dan forma a las transacciones actuales. No obstante, el incesante cambio tecnológico es redundante en la siguiente paradoja: al tiempo que se facilitan gran cantidad de transacciones, aparecen nuevos (y a veces mayores) riesgos que los anteriores. En este sentido, es notorio que en el Ecuador –como se señala en el artículo central de este boletín– la discusión sobre la seguridad en el mundo virtual es incipiente.

Las medidas de seguridad en el ciberespacio se efectúan a varios niveles. Un primer nivel es el concerniente a las precauciones que toman los usuarios en el uso de las TIC, principalmente al momento de realizar transacciones vía Internet o simplemente al navegar en la red. La cualificación del usuario es la principal medida en este nivel, e implica reconocer que el uso de la tecnología no es inocuo, sino que implica exponerse a ciertos riesgos que pueden y deben evitarse. En este ámbito son importantes los procesos de socialización y democratización de la tecnología a fin de contar con usuarios de Internet capaces de identificar el sinnúmero de mecanismos de fraude electrónico que existen.

Un segundo nivel de intervención está en las instituciones y empresas que desarrollan servicios *on-line*. El cumplimiento, por parte de estas instancias, de los protocolos de seguridad para transacciones electrónicas es fundamental. Los dispositivos de seguridad deben considerarse parte del servicio ofrecido, de tal manera que puedan establecerse responsabilidades en casos en que se compruebe negligencia en relación a delitos de esta naturaleza. En la mayoría de países de la región, se responsabiliza exclusivamente a las víctimas de los hechos que los agravian, desconociendo que el ciberespacio es una nueva esfera de las relaciones sociales y, por tanto, que la existencia de páginas *web* fraudulentas es un problema público y no un error individual. En este aspecto habría que indagar acerca del rol que cumplen en esta tarea de control las instancias destinadas a la protección del consumidor y de los usuarios como espacios de presión civil sobre las empresas y organizaciones que mantienen servicios en Internet.

Finalmente, este trabajo corresponde al campo penal con respecto al control de los delitos que se cometen gracias a la manipulación de las herramientas informáticas. En el caso del Ecuador, puede destacarse el esfuerzo de la Fiscalía a través de la Unidad de Delitos Informáticos como entidad especializada en el tratamiento de estos hechos. No obstante, se requiere una revisión profunda de las articulaciones entre los nodos del sistema penal (policía, justicia y cárcel), pues es bien conocido en el país que la existencia de normativas y dependencias no es suficiente para el cumplimiento efectivo de los derechos