www.flacsoandes.edu.ec

44

2011

Ciudad Segura

PROGRAMA ESTUDIOS DE LA CIUDAD FLACSO - ECUADOR

DELITOS INFORMÁTICOS

EDITORIAL
Página 1

ENTREVISTA
Delitos informáticos: mucho más cercanos que la ciencia ficción
José Luis Barzallo
Página 2

Delitos informáticos contra la intimidad
Gissela Echeverría
Página10

INTERNACIONAL
Sanciones para los ciber-delincuentes
Noemí López
Página 3

TEMA CENTRAL
Seguridad ciudadana en el ciberespacio
Enrique Mafla
Página 4

MEDIOS
Conflictos mediáticos y políticos
Rosa Enríquez Loaiza
Página 12

COMPARANDO
Página 9

POLÍTICA PÚBLICA
El control del ciberespacio
Alfredo Santillán
Página 11

SUGERENCIAS
Página 11

CORTOS
Página 3

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

ENTREVISTA

Delitos informáticos: mucho más cercanos que la ciencia ficción

José Luis Barzallo
Barzallo & Barzallo Abogados
Presidente de la Asociación Ecuatoriana de Derecho Informático
Autor del libro *La propiedad intelectual en Internet*

Para muchas personas, hablar de delitos informáticos les parecerá ciencia ficción. Para empezar la entrevista nos gustaría que introdujera al lector en esta temática.

Los delitos informáticos se han cometido desde hace varios años atrás. Como una anécdota, hace aproximadamente 25 años, en una de las películas de Superman, un delincuente dio las instrucciones para que un centavo de cada cuenta de un banco sea desviado a su cuenta. Estamos hablando de un acto delictivo que tiene como mínimo 25 años. Originalmente, los delitos informáticos aparecieron para obtener información. Estos datos personales se utilizaban para hacer ataques bancarios. Vale la pena aclarar que los delitos informáticos son los que se dan a través de las redes electrónicas, ma-yoritariamente en la Internet. Digo mayoritariamente porque también hay delitos en los cajeros automáticos, en donde los perjudicados son los bancos y los clientes del banco.

¿Cuáles son los delitos informáticos más comunes?

Los delitos informáticos se han perfilado, en su mayoría, hacia el phishing y a los ataques personales que sufren los individuos di-rectamente a través de los me-dios electrónicos. El phishing es la obtención de datos financieros o económicos a través de un engaño. Los ciber-delincuentes utilizan esta información para hacer una transferencia ilícita de fondos. Otro de los casos más comunes es el ataque a la honra o dignidad de las personas a través de las redes sociales como Facebook o Hi5. También suele pasar que se obtiene información de la persona para posteriormente cometer otro tipo de delito, como un secuestro, por ejemplo.

Nos habló un poco sobre el *phishing*. ¿Qué otras modalidades de delitos informáticos hay?

Las modalidades de delitos informáticos son las formas de describir las diferentes conductas o actos delincuenciales. Por ejemplo, la inclusión de un programa que desvíe todas o algunas de las llamadas entrantes a una empresa de comunicaciones IP (Internet Protocol) a un receptor ajeno a la empresa. También puede ser la conducta delictiva que utiliza un programa informático para que pequeñas cantidades de dinero sean transferidas a otras cuentas. *Phishing, tampering, spoofing, looping, flooding, campering, data dialing, lamming, zippering*… cualquiera de estas modalidades son simplemente los nombres que se les han puesto a los actos delictivos. Hay otra técnica conocida como el salchichón, que toma el nombre precisamente del *hot dog*, ya que consiste en la introducción de un programa espía camuflado en una información. Se puede utilizar también los famosos caballos de Troya para ocultar un programa determinado o una bomba lógica que hace el vaciamiento de toda la información. El objetivo final de todas estas modalidades es obtener información o algún beneficio económico a través de la inclusión de ciertos programas en los sistemas, más allá de la espectacularidad de sus nombres.

> *La Policía no tiene mucho margen de acción. Cuando llega uno de estos casos a la Fiscalía, se le pide a la Policía que investigue, pero al iniciarse este proceso, las partes ya han llegado a un acuerdo.*

¿Quién es el ciber-delincuente?

Afortunadamente, en la legislación ecuatoriana ya se contempla la figura del ciber-delincuente. Esto quiere decir que éste puede ser sancionado. El problema en nuestro país es que los ataques se producen casa adentro, lo que significa que el ci-ber-delincuente está dentro de la empresa o institución que ha sido perjudicada. Es gente que tiene acceso a los sistemas y sabe cuándo y cómo cometer el delito. Esto se da en los bancos, por ejemplo. El individuo transfiere a su cuenta pequeñas cantidades desde las cuentas del banco, cantidades que al final pueden sumar 300 mil, 500 mil dólares. Cuando el banco se da cuenta, se acuerda un calendario de pagos entre las partes en la Fiscalía y ahí queda todo. Este silencio beneficia al banco porque no se ve expuesto a publicidad negativa: lo que le in-teresa es que se devuelva el dinero más allá de una sanción.

Entonces, ¿no es común que los perjudicados denuncien el hecho en la Fiscalía?

No es común. Los pocos casos que llegan a la Fiscalía son aquellos en los cuales el perjuicio puede pasar de un millón de dólares, pero inclusive en estos casos se llega a un acuerdo y de ahí no pasa. No se llega a ningún juzgado.

¿Qué hace la Policía? ¿Se ha aplicado ya alguna sanción por delito informático?

La Policía no tiene mucho margen de acción. Cuando llega uno de estos casos a la Fiscalía, se le pide a la Policía que investigue, pero al iniciarse este proceso, las partes ya han llegado a un acuerdo. Las investigaciones realizadas hasta ahora han estado a cargo de la Unidad de Delitos Informáticos de la Policía, y precisamente esas investigaciones son las que han determinado que las personas que actúan en esto son gente de las propias instituciones afectadas. Sobre casos juzgados y sancionados, hay dos o tres. Uno por injurias realizadas por Internet y otro por la manipulación de los datos de migración. En ambos casos las normas sobre derecho informático no se han manejado correctamente durante el proceso.

¿Solamente se tipifica como delito informático aquel que utiliza Internet para hacer un uso doloso de la información?

No es solamente el uso doloso, ya que puede darse la simple obtención de información, como el caso de los *hackers*, que no son ningunos santos. El *hackerismo* es la obtención de información sin consentimiento. Hay algunos *hackers* que

obtienen la información y dicen que no le hacen daño a nadie, pues argumentan que es para consumo propio. Ante eso, siempre pongo el ejemplo de una persona que llega a su casa, ve que han entrado y lee un cartelito que dice "Señor: cambie de cerrajero por que sus chapas son malas". La información es privada. En el caso de las empresas, es información que puede estar bajo secreto empresarial. Desde diferentes perspectivas, la actividad del *hacker* debe ser considerada al menos ilícita, sino ilegal, tal cual sucede en la mayoría de legislaciones, por lo que ya tiene una sanción. El primer delito es la obtención de los datos y el segundo es utilizar esos datos para un delito concreto, ya sea en Internet o fuera de él.

Un delito que puede ser más grave que el propio delito informático…

En ese caso, el delito sigue siendo el mismo, lo que ha cambiado es el camino para cometer el delito: ahora se utiliza Internet para obtener información.

¿Cuál ha sido el caso más sonado de delito informático?

Fue un caso en el cual las personas de Migración habían hecho un cambio en el sistema para poderlo modificar, particularmente en lo relacionado al estado migratorio: un acto que fue identificado y sancionado.

¿Falta capacitación en el sistema judicial para abordar estos delitos?

Efectivamente. La Fiscalía dispone de un manual sobre peritaje informático. Este manual sirve cuando se presenta un caso en el cual hay que ir, revisar las máquinas y acceder a los sistemas. Parte del problema es que los juzgadores han aplicado la normativa sobre delitos informáticos de una manera bastante empírica. A manera de símil, se comete un delito ecológico en un río, pero los juzgadores asimilan una figura que está contemplada para una piscina. Los conceptos emitidos durante el juzgamiento no compaginan con la legislación vigente

Nicanor Benítez

En corto

- El *sexting* es una práctica que consiste en el intercambio de imágenes o videos de contenido erótico a través de los celulares. El problema radica en que se ha hecho bastante popular entre niños y adolescentes. Los datos muestran que cerca del 20% recurren a esta práctica y, de este porcentaje, un 80% son menores de 18 años. El 60% asegura haberlo enviado a su novio o novia, y un 11% admite haber enviado este contenido a otra persona.
- En México, los delitos informáticos han aumentado en un 22% desde el 2005. Uno de los delitos más frecuentes es el robo de información personal. El hurto de datos personales lo efectúan en un 85% delincuentes profesionales, 12% empleados y 2% hackers. Los datos más requeridos por los delincuentes son cuentas bancarias, tarjetas de crédito, identidades completas, cuentas de subastas en línea, *mailers*, direcciones de correo y contraseñas.
- En octubre de este año, la Guardia Civil española puso en marcha "Yo denuncio", una campaña de concienciación y colaboración entre los usuarios de redes sociales. Ofrece a los internautas la posibilidad de denunciar un delito informático, además de dar información sobre diferentes delitos en la red y las modalidades más habituales utilizadas por los delincuentes. La campaña inició en Facebook, superando ya los siete mil amigos. En Twitter el número de seguidores ha sobrepasado el millar.

Internacional

Sanciones para los ciber-delincuentes

Noemí López

El 4 de junio de 2008, la Cámara de Diputados de Argentina sancionó la Ley 26.388 de Delitos Informáticos, con la finalidad de tener una regulación legal que permita sancionar con multas y prisión a quienes cometan algún crimen informático. Esta ley modifica, sustituye e incorpora figuras típicas a diversos artículos del Código Penal, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el mismo. A lo largo de su articulado, la ley tipifica varios delitos informáticos como pornografía infantil, violación, apoderamiento o desvío de comunicación electrónica, intercepción o captación de comunicaciones electrónicas, acceso a un sistema o dato informático, publicación de una comunicación electrónica, acceso, revelación o inserción de datos falsos a un banco de datos personales, fraude, daño o sabotaje informático.

El debate tendiente a minimizar las lagunas jurídicas que existían en el ordenamiento nacional respecto a los delitos producidos a través de las nuevas tecnologías de la información (TIC) comenzó en el 2000 con la promulgación parcial de la ley de Habeas Data (25.326), de Protección de Datos Personales, donde también se protegen las bases de datos informáticas. Con las modificaciones al Código Penal del 2008 se reconoce la validez de los documentos y las firmas digitales como equivalentes a los documentos en cualquier otro soporte, a la vez que se reconoce la privacidad e inviolabilidad del correo electrónico, colocándolo a la misma altura que el correo epistolar.

El primer estudio que se realizó en el país a raíz de la aprobación de la Ley 26.388 fue un informe privado preparado por la consultora Ernst & Young, la cual realizó una encuesta a 115 compañías radicadas en Buenos Aires. Esta reveló que, en el 2008, un 73% de las empresas fue víctima de algún delito digital, 19% de esos ilícitos se vincularon con defraudaciones (manipulación y acceso de datos, *phishing* o *pharming*), mientras que el 10% correspondió a delitos extorsivos y el 8% se relacionó con el correo electrónico[1]. El 54% de las compañías investigó los delitos, pero en la mayoría de los casos no se pudo identificar al autor, ya que sólo en 25% de los procesos se sabe quién es el responsable.

El coordinador de la Comisión de Derecho Informático del Colegio Público de Abogados de la Ciudad, Hugo Sorbo, estima que por cada cuatro delitos informáticos solo uno se denuncia. Además informó que "los delitos informáticos, especialmente el acceso indebido y la violación de *e-mails* por ex parejas o compañeros de trabajo, están creciendo, pero al mismo ritmo aumenta lo que se conoce como 'cifra negra', que son los casos que no se denuncian"[2]. En los últimos dos años y medio, el poder judicial porteño contabilizó 8.425 denuncias por ciber-delitos. Se estima que las consultas desde que se sancionó la Ley 26.388 crecieron entre un 30% y 50%, y que la acusación más frecuente se centra en el robo de claves de casillas de *e-mail* para suplantar identidades.

Como parte de ratificar su política contra los ciber-delitos, Argentina se adhirió formalmente a la Convención de Budapest, que cuenta actualmente con la suscripción de 43 países y la ratificación de 23 de ellos, y prevé la cooperación internacional en la lucha contra crímenes informáticos. Además brinda un marco veloz y seguro de cooperación y colaboración internacional para la persecución de delitos informáticos transnacionales, por lo que la participación del país permite la cooperación de fuerzas de los distintos países y el asesoramiento de expertos técnicos

1 Iprofesional.com (s/f). "El 73% de las empresas declaró ser victima de un delito informático". Disponible en <http://www.iprofesional.com/notas/76123-El-73-de-las-empresas-declaro-ser-victima-de-un-delito-informatico.html?cookie>, visitado el 25 de octubre de 2010.
2 El Clarín (2010). "Solo se denuncia uno de cada cuatro ciberdelitos". Disponible en <http://www.clarin.com/internet/mundo_web/Solo-denuncia-ciberdelitos_0_280172032.html>, visitado el 2 de noviembre de 2010.