www.flacsoandes.edu.ec

44

2011

Ciudad Segura

PROGRAMA ESTUDIOS DE LA CIUDAD FLACSO - ECUADOR

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 dali ng*); fraudes, daños y sabotajes financieros (ej.: *phi shi ng* o *pha rmi ng*); acosos y abusos a infantes y adolescentes (ej.: *sexti ng, groomi ng* o *bullyi ng*); ataques a infraestructuras de gobiernos y organizaciones (ej.: *hacki ng*); extorsiones y suplantaciones (ej.: *spoofi ng*); 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

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

FLACSO ECUADOR

ENTREVISTA

Delitos informáticos contra la intimidad

Gissela Echeverría
Consultora en Comunicación, Familia y Sexualidad

¿Cómo la delincuencia informática puede atentar contra la intimidad de las personas en su vida cotidiana, en particular denigrando sus relaciones interpersonales? ¿Cuáles son los delitos informáticos que afectan este ámbito?

Existen varios. Los que más me preocupan son los relacionados con la integridad de niños y adolescentes. Existen espacios de foros, salas de *chat* o incluso el Facebook que son utilizados, por ejemplo, como mecanismos para hacer *bullying* (acoso escolar). Los agresores entran a los muros de Facebook e insultan a un niño o adolescente, lo denigran y lo desprestigian. Esa es una forma de acoso que maltrata al individuo. Otra de las formas es el famoso *grooming*, que se da cuando un adulto con apetencia sexual por jovencitos se hace pasar por una persona de la misma edad para establecer una relación con el adolescente, y luego inducirlo a tener iniciación sexual (con masturbación, por ejemplo) a través de una cámara *web*, mientras el adulto observa y da instrucciones. En ese caso, aunque sea de manera virtual, tenemos tanto acoso como abuso. También existe el llamado *sexting*, que consiste en el envío de mensajes con contenido pornográfico por celular o correo electrónico. Por ejemplo, se han dado casos de parejas adolescentes que mantienen relaciones sexuales, las filman y luego publican ese material en las redes sociales o lo envían por correo electrónico.

El uso que se le está dando a este medio deja entrever una falta de conciencia de los límites del respeto a los derechos de privacidad e intimidad de las personas, los cuales se ven vulnerados.

Todo esto termina significando una ruptura del concepto de privacidad. El uso que se le está dando a este medio deja entrever una falta de conciencia de los límites del respeto a los derechos de privacidad e intimidad de las personas, los cuales se ven vulnerados. En muchos casos, el Internet se está utilizando como un mecanismo para aprovecharse de la inocencia o ingenuidad de los menores, y también como forma de violencia entre personas adultas para cometer venganzas o distribuir públicamente información privada. Ante esto, se debe tener en cuenta que cada avance tecnológico, si bien puede significar un gran progreso, también implica riesgos para los seres humanos, riesgos que vienen dados por su mala utilización, o por la utilización con fines de depredación o con fines fuera de la ética y el respeto a las personas.

¿Son frecuentes en el Ecuador los casos de este tipo de delitos informáticos? ¿En este sentido, se trata de un problema serio en nuestro país?

Claro que lo es. A veces se piensa que en el Ecuador, como el nivel de conectividad es bajo, entonces el acceso también lo es. Sin embargo, una cosa es la conectividad y otra muy diferente el acceso que la gente tiene al Internet. Los porcentajes de este último son muy superiores: mientras la conectividad está entre el 10 o 12%, el acceso está por encima del 50%. Esto quiere decir que existe una gran incidencia del problema. Hace poco yo traté un caso de una adolescente que fue secuestrada gracias a la información que ella mismo había publicado en el Facebook. Es muy común que la gente ponga todo tipo de información en las redes sociales, información que incluye señales de localización y ubicación, incluso información relevante con respecto a su casa, su dirección, sus rutinas y hábitos, con lo cual se ponen a sí mismos en una circunstancia de vulnerabilidad frente a alguien que podría causarles daño. Esto está pasando todo el tiempo, pero por lo general no sale a la luz pública. Por eso nuestra preocupación principal debe ser alertar a jóvenes y adultos sobre el problema.

¿Qué métodos y precauciones debemos tomar para evitar ser víctimas de este tipo de riesgos?

Hay que comprender que el medio es siempre un instrumento. El medio no es bueno ni malo por sí mismo, pues eso depende de la utilización que le demos. Por tanto, la indicación es reflexionar sobre el tipo de uso que le estamos dando al Internet, y hacerse las preguntas que son de responsabilidad individual: ¿Qué necesidad tengo de publicar en Facebook una fotografía en la que aparezca besándome con mi pareja? ¿Qué es lo que intento comunicar con eso? ¿Para qué necesito que todo el mundo se entere de mi privacidad? ¿Es ético? ¿Es justo? ¿Es respetuoso de mí mismo?, etc.

Por otro lado, como padres, como adultos, tenemos que involucrarnos en el control del tiempo de utilización del Internet por parte de nuestros hijos. Es necesario verificar qué tipo de páginas están utilizando, implementar los controles parentales (para bloquear páginas de pornografía, por ejemplo), permitir a los hijos que tengan correo electrónico pero con una clave que los padres conozcan (para eventualmente revisar su actividad), etc. No se trata de invadir, sino simplemente de asumir una responsabilidad, pues mientras sean niños y adolescentes dependen de nuestra vigilancia para su propia seguridad y protección. También es necesario prevenir a los jóvenes de los riesgos que existen y motivarlos a hablar sobre el tema

Andrés Landázuri