



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 límites, 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 diali 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 incumplimiento 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 intimidación
Gissela Echeverría
Página 10

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 Loiza
Página 12

COMPARANDO
Página 9

POLÍTICA PÚBLICA
El control del ciberespacio
Alfredo Santillán
Página 11

SUGERENCIAS
Página 11

CORTOS
Página 3

