PROYECTO UNAM

Coordinador: Roberto Arturo Gutiérrez Alcalá **robargu@hotmail.com**

¿Para qué un observatorio atmosférico en la azotea?

El Seminario del Centro de Ciencias de la Atmósfera y de El Colegio Nacional invitan a la conferencia "¿Para qué un observatorio atmosférico en la azotea"? que impartirá el doctor Michel Grutter de la Mora mañana viernes 21 de septiembre, a las 12:00 horas, en el Auditorio Julián Adem Chahín, del mencionado centro, en Ciudad Universitaria

ARCHIVO EL UNIVERSAL

REZAGOS EN LA TIPIFICACIÓN Y PERSECUCIÓN DE

DELITOS INFORMÁTICOS

El país carece de policía, agentes del Ministerio Público, abogados y jueces suficientemente preparados para enfrentar las conductas delictivas perpetradas por medios electrónicos

México ocupa el último lugar en materia de ciberseguridad dentro del grupo de países que integran la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

Está rezagado en cuanto a la tipificación de los delitos informáticos se refiere y no cuenta con recursos humanos suficientemente preparados para combatirlos con eficacia, como policías investigadores, agentes del Ministerio Público, abogados y jueces.

De este modo, los ciberdelincuentes siguen haciendo de las suyas con total impunidad: cometen fraudes electrónicos, lavan dinero, roban o venden bases de datos, clonan tarjetas bancarias, bloquean portales gubernamentales –especialmente del gobierno federal– o, peor aun, participan en el negocio de la pornografía infantil.

¿Qué hacer, cuáles son los delitos cibernéticos más frecuentes en el país y por qué no están regulados? A esas y otras interrogantes responde Julio Téllez, investigador del Instituto de Investigaciones Jurídicas de la UNAM y especialista en derecho y nuevas tecnologías.

"México es uno de los países donde hay más pornografía infantil, es decir, donde se obliga o induce a niños, niñas y adolescentes a realizar actos sexuales lesivos por medios electrónicos como la Internet. A pesar de ello, oficialmente se habla poco de este delito. Se oculta también mucho el *ciberbullying*, conducta de acoso entre iguales, en este caso menores de edad, a través de medios electrónicos, que sin duda amerita discusiones y regulación especial por las graves consecuencias (suicidio, por mencionar una) que puede acarrear entre los agredidos y sus familiares", dice.

Para el investigador universitario, la pornografía infantil va ligada al *sexting* (contracción de *sex* y *texting*), término que nombra la generación o el envío de contenidos eróticos o sexualmente explícitos que están en la frontera de lo pornográfico, y al *grooming*, palabra que alude al hecho de que un adulto se haga pasar por un menor de edad con la finalidad de ganarse poco a poco la confianza de otr^ menor y posterio: mente concert: una cita con él pa: cometer una co: ducta delictiva rel: cionada con la po nografía infantil, trata de personas el secuestro.

Otro delito se as: cia al secuestro d: infantes: a muchos de los que han sido privados de su libertad se les videograba mientras muestran sus genitales, son sodomizados o sostienen relaciones sexuales con menores de edad, adultos e incluso animales.

"En ocasiones se presentan actividades aun más execrables, como asesinarlos después de haberlos videograbado, para cercenarlos, extraerles sus órganos vitales y vender éstos en cantidades estratosféricas. Sobre el lucrativo tráfico de órganos, buena parte del cual se origina a partir de la problemática del secuestro de infantes, la trata de menores y la pornografía infantil, las autoridades suelen ser omisas. Casi no se habla de este delito en México", asegura Téllez.

Spam, fishing...

El *spam* (correo electrónico no deseado o solicitado) es también frecuente en nuestro país. Puede ser *fishing* (un anzuelo para los usuarios) o *farming* (un simulador).

El *fishing* nos pide información para actualizar una supuesta base de datos, lo cual permite al ciberdelincuente acceder a nuestras cuentas bancarias y vaciarlas.

El *farming* nos conduce a un portal que simula ser el de nuestro banco, donde otra persona sustrae nuestros recursos financieros.

Otro de los delitos recurrentes que ha sido observado por el investigador de la UNAM es la clonación de tarjetas bancarias.

Es común que, de repente, en los estados de la cuenta bancaria de una tarjeta de crédito o débito de una persona o empresa haya disposiciones en efectivo o compras no efectuadas por el titular, sino por personas ajenas que clonaron o vendieron los clones de dicha tarjeta.

"El lavado de dinero también se está dando cada vez con más frecuencia en México. Ante las disposiciones más restrictivas emitidas por las autoridades hacendarias del país, los que tienen dinero mal habido recurren ahora a subterfugios electrónicos para lavarlo", señala Téllez.

Usurpación de identidad

En México, como en otros países, muchos delitos informáticos no están tipificados como tales en el Código Penal, debido a los constantes cambios que ocurren en el mundo de la tecnología. Además, enfrentamos el reto de las distintas codificaciones penales que marcan las jurisdicciones locales ante un problema que no es sólo nacional, sino global.

"El *spam* es uno de esos delitos. Vía correos electrónicos o redes sociales se busca infiltrar *spyware*, programas que se alojan en nuestra computadora y permiten a un ciberdelincuente controlarla a distancia."

Además de tener acceso a toda nuestra información, el ciberdelincuente puede usar nuestra computadora como una especie de miniservidor para enviar *spam* o virus informáticos a otras computadoras sin que nos demos cuenta.

En cambio, la usurpación de identidad es un delito informático que recientemente se tipificó como tal en el Distrito Federal, el Estado de México y Colima.

"Consiste en obtener información personal que alguien subió a las redes sociales o a otro sitio de la red, y ostentarse como ese individuo para delinquir, ya sea mediante la extorsión, el chantaje, el secuestro u otra actividad ilícita", explica el investigador.

Impunidad

¿Cómo hacer frente a esta moderna delincuencia? En la actualidad, muchos de los delitos informáticos se manejan bajo un esquema de impunidad. De ahí que, en principio, sea clave tipificarlos. Si no están tipificados en un Código Penal (federal o local), no son delitos y, por consiguiente, no pueden sancionarse.

Asimismo, de nada sirve tener una tipificación en México, si dichos delitos informáticos no están regulados en otros países. No se puede olvidar que la extraterritorialidad (un principio del Derecho Público Internacional) impide aplicar una ley nacional en otro país.

"Por eso, todos los países tienen que ponerse de acuerdo para regular los delitos informáticos. Y es necesario que, una vez tipificados, las autoridades sepan cómo investigarlos y los jueces estén preparados y tengan la capacidad de valorar las pruebas presentadas para aplicar sentencias."

> El *spam* es uno de esos delitos. Vía correos electrónicos o redes sociales se busca infiltrar *spyware*, programas que se alojan en nuestra computadora y permiten a un ciberdelincuente controlarla a distancia"
>
> **Julio Téllez,** investigador del Instituto de Investigaciones Jurídicas de la UNAM

Según el investigador de la UNAM, se debe contar también con más y mejores equipos tecnológicos, y con más grupos de policía especializada que puedan perseguir y atrapar a los ciberdelincuentes.

"Si bien la PGR y algunas procuradurías generales de justicia estatales como la del Distrito Federal tienen grupos de policía especializada para combatir la ciberdelincuencia que han alcanzado ciertos logros, la Policía Cibernética de la Secretaría de Seguridad Pública Federal se ha visto acotada últimamente en sus funciones, por lo que se requiere una mayor colaboración", indica.

Propuestas

Aunque la UNAM cuenta con el Equipo de Respuesta a Incidentes de Seguridad Informática (conocido con las siglas CERT-UNAM), en opinión de Téllez, éste podría tener, además, un laboratorio de informática forense, abocado a identificar y dar elementos o peritajes para fincar responsabilidades a los ciberdelincuentes, a quienes es difícil seguirles la pista.

Ante la vulnerabilidad en materia de seguridad nacional y seguridad pública debida a la impunidad en la comisión de delitos informáticos, Téllez hace esta proposición: "Hay que emprender acciones y reformas legislativas, destinar más recursos tecnológicos para la investigación forense, así como para la formación de policías investigadores, agentes del Ministerio Público y jueces especializados. Solamente así podremos enfrentar esta nueva forma de delincuencia que, además de estragos en el orden patrimonial, puede ocasionar una enorme desestabilización en el país."(Fernando Guzmán Aguilar)

LOS IMPLICADOS

EL CIBERDELINCUENTE: Generalmente es muy joven e inteligente, y aprovecha los errores y la falta de cuidado de los usuarios o funcionarios públicos, así como las falencias en los sistemas de seguridad de instituciones o dependencias gubernamentales, y las deficiencias en los planes de atención de contingencias.Los menores infractores, como les llama la ley, son motivo de un tratamiento penal diferenciado, con sanciones más atemperadas en relación con los delincuentes adultos propiamente dichos, por lo que se tornan doblemente peligrosos por su habilidad e impunidad. Téllez es de la idea de que hay que poner penas ejemplares para evitar que más jóvenes engrosen las filas de la delincuencia informática. Pero lo más importante es generar una cultura informática adecuada para que todos los usuarios de medios electrónicos tomen sus precauciones y protejan su información.

LA VÍCTIMA: Aparte de sufrir daño patrimonial porque clonaron su tarjeta bancaria y perdió sus recursos financieros, la víctima padece una especie de daño moral. No es objeto de protección adecuada por parte de las autoridades y bancos (en contadas ocasiones, éstos le devuelven el dinero perdido). El usuario de celulares, computadoras y otras tecnologías debe tomar ciertas medidas de seguridad, pero quienes lo invitan a "usar la modernidad" tienen que protegerlo también o, en un momento dado, compensarlo en caso de haber sido víctima de esta nueva pero cada vez más creciente delincuencia.