La era de los CIBERDELITOS

DIEGO MIGLIORISI es especialista en derecho informático y autor de *Crímenes en la web*. Explica claramente los tipos de estafas que existen en la red de redes y qué dice la ley sobre cada uno de ellos

POR Florencia Álvarez

–¿Cuál es el objetivo de haber escrito este libro? En los últimos cinco años se ha gestado un vertiginoso avance de Internet sobre la sociedad y por ende sobre las acciones de la personas y empresas, comprendiendo resultados netamente positivos tanto en la comunicación globalizada como también en el potenciamiento de derechos fundamentales para la humanidad como la libertad de expresión, la libertad de prensa y la libertad de acceso a la información, entre miles de cualidades positivas que trajo esta invención histórica. Pero la otra realidad se presenta cuando la mente criminal hace uso de estas herramientas para cometer delitos. Por lo tanto consideré importante contarle a la sociedad cuál es el otro lado de la web y la amenaza que ello representa.

–¿Cuál es el crimen informático más común en nuestro país? Es importante aclarar que los delitos informáticos se clasifican por un lado en "propiamente informáticos", son los que nacieron con la web: *hacking*, daño informático, *phishing*, *typosquatting*, *cyberquatting*, *mettatanging*, etc., y por otro lado, existen los delitos tradicionales del Código Penal que se configuran a través de Internet. Estos últimos enmarcan un 80% de los delitos informáticos. Aquí los delitos más frecuentes son: amenazas, calumnias, extorsión y acoso en todas sus variantes.

–¿Quiénes pueden ser víctimas de estos delitos, y cuáles son las características de las personas que los llevan a cabo? Cualquier persona puede ser víctima de un delito informático, incluso quienes no utilizan Internet. Hay cientos de delitos, por lo tanto el modus operandi varía en cada caso. En referencia a quienes los producen, pueden ser personas con amplios conocimientos informáticos, pero en la mayoría de los casos son simplemente usuarios con conocimientos básicos.

–¿Entrar sin autorización a determin dos sectores de

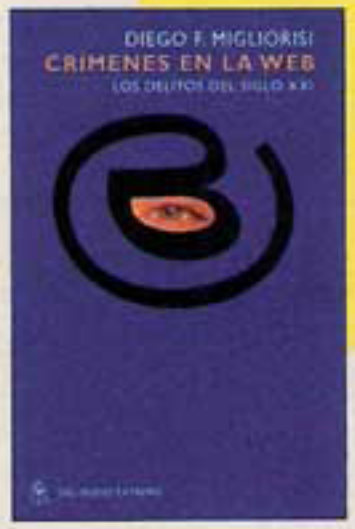
una web, o abrir una cuenta de e-mail ajena es considerado un crimen? Sí, claro, el acceso indebido es un delito penado en la Argentina y en casi todos los países del continente. De hecho, si nos fuéramos a África, Angola o Senegal por ejemplo, también es delito. Lo mismo ocurre en Europa. De hecho, si observamos legislaciones de países muy lejanos de la Argentina como Mongolia, Buthan, Kazajistán o Timor Oriental, vemos que tienen legislación clara y precisa, y el acceso indebido también es considerado un delito.

–¿De qué manera está penado por la ley? En la Argentina, dependiendo del caso, la pena puede ir entre quince días hasta el año de prisión. En cambio, la legislación venezolana contempla hasta cinco años de prisión, el Código Penal de la República de Mozambique contempla prisión de hasta ocho años, por citar algunos ejemplos. La cuestión fundamental, y lo más difícil, es cómo probar el delito.

–¿Cómo se valora en Argentina el hurto de información? En la Argentina no está tipificado el hurto informático, sólo el acceso indebido se contempla como delito. Para la legislación argentina al no existir tangibilidad de la cosa, no existe hurto. En cambio, otros vecinos latinoamericanos se aproximan a dar una solución a este tipo de situaciones. En Perú, Honduras o Venezuela, el robo de información mediante sistema de transferencia electrónica está tipificado en su código al hurto informático de forma literal.

–¿Cómo actúan los instigadores al cibersuicidio? Como en la vida fuera del ciberespacio. Dentro de la web conviven grupos, páginas, perfiles destinados a colaborar con personas que dudan en tomar este tipo de decisiones. En algunos casos enseñan diferentes técnicas para configurar el suicidio, en otros además incitan al suicida psíquicamente para que tome la decisión. En el libro se relatan algunos casos alrededor del mundo.

–¿Qué dice la ley local sobre la delincuencia informática? Tanto en la Argentina como en la mayoría de los países del mundo existe tendencia de adaptación de los delitos informáticos a las diferentes legislaciones penales. En algunos países las penas son más duras y en otros más leves, pero en definitiva el mundo va reaccionado ante esta nueva amenaza que nos trae el siglo XXI. El siguiente paso debería darse con un ordenamiento de coordinación globalizado en materia probatoria. Tengamos en cuenta que Internet no tiene fronteras y la prueba de un delito cometido en determinado lugar puede estar en cualquier parte del mundo.



–¿Qué papel cumplen los buscadores en los ciberdelitos? En principio no cumplen ningún papel en la cadena delictual. Los buscadores son como bibliotecas virtuales que indexan información cargada por usuarios y dan links de respuesta a requerimientos de búsqueda. La justicia, en muchos casos, ordena desindexar de los resultados búsquedas que afecten a determinada persona o que tengan contenido delictual. Vale señalar que la desindexación será dentro del ámbito local solamente.

Si bien los buscadores ejercen lo que denominamos autorregulación mediante sus terminados y condiciones de uso (hay páginas con notorio contenido delictual que son desindexadas por sus propias políticas), no pueden contra la libertad de expresión y el acceso de información. Por la tanto es la justicia quien debe ordenar la desindexación.

–¿Qué tipo de nuevos delitos se han visto favorecidos a partir de la llegada de las redes sociales? Las calumnias principalmente, también la amenazas. La usurpación de identidad, y desde ya las diferentes modalidades de acoso conocidas como *bullying* o *grooming*.

–En su opinión, ¿de qué manera se debería controlar la red de redes para detener estos crímenes? La problemática es tan profunda como la web, y la decisión debe ser global, no sirve de mucho tomar una medida en un país y en otro no. Algunas de las medidas que colaborarían en la lucha contra este tipo de delito son: la verificación real del creador del perfil, el guardado de tráfico local (con las debidas protecciones al derecho a la intimidad), y el guardado de información de conexión por parte de las redes sociales que es el IP de usuario y demás ■

Los nombres de la ilegalidad

Hacking: es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, sus vulnerabilidades y la forma de aprovecharlos para delinquir.

Typosquatting: es una técnica basada en los eventuales errores tipográficos en que puede incurrir un internauta a la hora de introducir en su navegador la URL de una página web. De este modo, a todo aquel usuario que accidentalmente introduzca una dirección web incorrecta, se le mostrará una información alternativa en un sitio distinto, gestionado por un cybersquatter.

Cyberquatting: es la acción de registrar un nombre de dominio, adelantarse a alguien que es dueño de una marca por ejemplo, con el propósito de extorsionarlo para que lo compre o bien simplemente para desviar el tráfico web hacia un sitio competidor o de cualquier otra índole.

Phishing: obtienen datos de tarjetas de crédito, claves y nombres de usuario a través del correo electrónico para suplantar la identidad de los clientes de bancos y acceder a cuentas de correo legítimas desde las cuales continuar la estafa.

Pharming: los timadores buscan vulnerabilidades informáticas en sitios web auténticos para poder direccionar las visitas que se realizan a estos hacia sus propias páginas. Desde ahí obtienen la información de las víctimas.

Spamming: es el abuso de cualquier tipo de sistema de mensajes electrónicos, mensajería instantánea, en foros, blogs, buscadores, mensajes, en teléfonos móviles, etc.

Hoax: son mensajes de e-mail con contenido falso o engañoso, impactantes, generalmente proveniente en forma de cadena. Los mensajes suelen tener características como pedir al lector que reenvíe el mensaje; amenazas de desgracias; pérdida de servicios y similares.