Evolución histórica de los delitos informáticos

Por Gustavo Sain
@grsain

La creación de nuevas tecnologías que intermedian en la comunicación entre las personas trae aparejado nuevas posibilidades para su aprovechamiento indebido e ilícito. Eso sucedió desde la creación del telégrafo y también posterior incorporación del teléfono a la vida cotidiana de las personas. Con la irrupción de la computadora personal y la posterior expansión de Internet y la World Wide Web; la capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo de características globales amplió las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales "amigables" y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto asi como las posibilidades de anonimato en las comunicaciones.

Los orígenes de los delitos informáticos pueden rastrearse a partir de los años 60s por el temor infundido por la literatura de la época en relación a la recolección y almacenamiento de datos personales en computadoras. Éste tiene como referencia la obra "1984" de George Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías. Tras la publicación de artículos periodísticos sobre algunos de los casos apareció por primera vez del término *delitos informáticos* o *delincuencia relacionada con computadoras***,** retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como "cyberpunk".

Durante los años ´60 en pleno Flower Power norteamericano, diferentes programadores o especialistas en informática intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio telefónico. El activismo político hippie de la época tuvo su costado informático a través de los *phreakers* (neologismo proveniente de las palabras en inglés *freak*, de rareza; *phone,* de teléfono; y *free*, gratis) donde a través de las

llamadas *blue box* o cajas azules establecían comunicaciones en forma gratuita simulando los tonos de llamadas utilizadas por la Bell Corporation y la ATT, básicamente para comunicaciones de larga distancia. Con el correr del tiempo, estas técnicas de hacking alcanzaron un mayor grado de sofisticación, utilizadas también para las manipulaciones de transferencias de dinero por redes telefónicas vulnerables. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales.

Ya durante la década de 1970 se comienzan a registrar una serie de casos que arrojan pérdidas cuantiosas para los sectores privados. A partir del desarrollo de delitos económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión. En relación al espionaje, estos se llevaban a cabo mediante la copia directa desde los dispositivos informáticos, el robo directo de los mismos para la extracción de información -discos duros, diskettes-, y la absorción de emisiones electromagnéticas para la captación de datos. Los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco espionaje industrial.

Para los casos de sabotaje y extorsión informática, estos eran los delitos que más preocupaban a las administraciones gubernamentales y empresas ante la alta concentración de datos almacenados electrónicos. Los objetivos eran tanto bienes tangibles -dispositivos físicos- como intangibles -datos e información- afectando tanto hardware como de software de los dispositivos. En relación a los daños físicos, durante los años 70s se registraron casos de uso de bombas caseras en instalaciones y dispositivos informáticos de empresas por distintos problemas laborales. En relación a los fraudes financieros producidos a partir del uso de nuevas tecnologías, los primeros casos se empezaron a producir en Estados Unidos a finales de la década de 1970 a partir de los fallos en los sistemas de seguridad de las redes y la inexperiencia de los administradores de dichos sistemas. El modus operandi se relacionaba

con la manipulación de facturas para pagos de salarios de personal y los balances de pagos de los bancos.

A partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. Esto motivó la utilización por parte de las empresas emisores de la adopción de chips en los plásticos como medida de seguridad. Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

A fines de esa década comenzaron a aparecer contenidos ilícitos y nocivos en las redes tales como amenazas contra las personas, incitación al odio y el intercambio de material de pornografía infantil, tanto así como actos de violencia y discriminación racista por parte de grupos extremistas. Nuevas técnicas de hacking manipulaban sistemas de vuelo o sistemas hospitalarios y de salud, definidos como “ataques contra la vida”. Estos hechos aumentaron significativamente a la par del incremento de usuarios de la red, haciéndose evidente a nivel gubernamental en 1989, cuando la justicia alemana identificó a hackers que utilizaban las redes de datos internacionales para el acceso a información privilegiada de Estados Unidos y Gran Bretaña para vender la información a la KGB.

Con la apertura global de Internet a mediados de los 90s por parte de la administración norteamericana y el posterior desembarco de las empresas y bancos a la red para el desarrollo del comercio electrónico, la preocupación central pasaba por el desarrollo de estándares de encriptación seguros para el desarrollo de operaciones financieras y la compraventa de productos en línea. Asimismo, la industria discográfica y cinematográfica

comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor a partir de la descarga e intercambio en línea de música y películas bajo leyes de copyright, lo que generó un debate acerca de cómo concertar acciones de cooperación internacional para evitar fugas del negocio. La difusión de imágenes y/o ofrecimiento de servicios sexuales de menores en la Web alertaban a las autoridades de los países sobre la ola de pedofilia que asomaba a partir de casos de grooming o acoso sexual a menores en línea. El tema de la protección a la intimidad y la privacidad se empezaron a debatir mediante el uso de nuevas tecnologías.