Ataques y delitos informáticos

José Gabriel Réding Domínguez
Jesús Alejandro Flores Hernández
Jorge Vázquez Torres*

Introducción

Los cambios tecnológicos se han venido suscitando de manera vertiginosa. Las computadoras, las redes, las telecomunicaciones y el acceso a la información se han convertido en los parámetros de la modernidad. La creciente ola de integración de las personas en la Internet ha traído como consecuencia la generación de una nueva cultura naciente en el intercambio de datos.

Los llamados cibernautas, la disposición y acceso a la información, han abierto la puerta al conocimiento de las computadoras y la facilidad con que adquirimos nuevas ideas nos está llevando a cruzar las fronteras marcadas por el derecho. Ahora debemos redefinir los límites de propiedad, sin considerar a ésta como algo tangible, ya que en la actualidad tenemos la propiedad virtual, propiciando un derecho y una obligación con nuevas características.

En este nuevo escenario científico, tecnológico y social, debemos entender que la sociedad está creando un nuevo poder, mismo que faculta a los versados en el tema, para la manipulación informática voluntaria e involuntaria, utilizando los recursos de cómputo en general; a este poder le podríamos llamar: *poder informático*.

La creciente acumulación de información en bases de datos, los grandes recursos de hardware y *software* cada vez más accesibles, así como la integración a gran escala de los componentes electrónicos han dado cabida a la aparición de gente con grandes capacidades intelectuales mal encaminadas, mismos que utilizan estos recursos para promover los llamados delitos informáticos, transgrediendo el derecho de otras personas en sus posesiones intelectuales o en ellos mismos.

Ahora bien, no todo es delito, debemos entender que el avance de la tecnología ha traído desde siempre, aspectos positivos y negativos, pero lo que en el presente artículo nos atañe es la necesidad de contar con una cultura y lineamientos para regular la transgresión y promover el respeto informático.

Palabras y frases clave: Transgredir, respeto informático, delito, informático, bases de datos, telecomunicaciones, redes, propiedad virtual, Internet, *phreaking*, *phone*, *freak*, *hackers*, poder informático.

Delitos informáticos

Al buscar el significado de la palabra delito, en un diccionario común o en uno enciclopédico, encontramos algo similar a: "conducta, acción u omisión tipificada (considerada) por la ley, antijurídica o contraria a derecho y con posibilidades de ser castigada o penada por las normas de la sociedad". Proviene del vocablo latino *delinquere* que significa apartarse del buen camino marcado por la ley.

Por otro lado, al referirse a la palabra informático encontramos que es un conjunto de conocimientos acuñados a partir de la *automatización de la información* a través de los ordenadores o computadoras. La palabra informático proviene del acrónico de *información* y *automático*.

El delito informático, crimen cibernético o electrónico, ha adoptado una versatilidad que incluye a las actividades ilícitas tradicionales como el fraude, la extorsión, la malversación de fondos, entre otros, pero más aún, ha adquirido matices revolucionarios que se vuelven cada vez más sofisticados.

Los ataques realizados por los *hackers*, la violación de los derechos de autor o el *phreaking* son actividades que se han vuelto comunes en nuestra sociedad. La mayoría de los sitios web, visitados por millones de personas en todo el mundo, están siendo constantemente actualizados en la búsqueda de brindar seguridad a sus clientes, no obstante parece ser que los delincuentes informáticos siempre encuentran medios técnicos y opciones tecnológicas para poder atacar a sus víctimas, mismos que en la mayoría de las ocasiones no se percatan del ataque.

Con el advenimiento de los sistemas de cómputo, las comunicaciones y por supuesto la globalización y eliminación de fronteras informáticas, se dio pauta al incremento en el uso de los servicios de TI (Tecnologías de Información). Desde siempre hemos contado con conductas antisociales y delictivas que ponen de manifiesto la inconformidad de los agresores en contra de la sociedad o de algún individuo en particular, pero el incremento en el uso de las computadoras, ha provocado un aumento en la incidencia en la comisión de los llamados delitos informáticos, estos que van desde el uso indebido de bases de datos, la modificación de archivos, el daño en el software o hardware, etc., poniendo de manifiesto la necesidad de regular sobre el tema de delitos informáticos y mantener esta legislación en constante actualización.

Lo más común es encontrar ataques hacia los sistemas de cómputo, tal vez bajo la bandera de que la mayoría de la gente tiene acceso a una computadora o a la red de las mismas; pero, por otro lado, el ataque a los sistemas telefónicos hecho por los llamados *phreakers* es de una complejidad un poco mayúscula, pues deben entender el sistema telefónico y el manejo de los aparatos y equipos para poder obtener beneficios de carácter ilegal. La palabra *phreaker* proviene de una contracción de *phone* (teléfono en inglés) y *freak* (miedo o monstruo). Los antecedentes conocidos de estos delitos se remontan al uso de artefactos conocidos como la *caja de queso* y más tarde la *caja azul*.

En los países de Europa y América del Norte se ha presentado un notable incremento en las actividades criminales que han sido enmarcadas como robos, hurtos, fraudes, falsificaciones, otros, de carácter informático. Desafortunadamente la lista es mucho más extensa y abarca daño inclusive en la propiedad intelectual.

Dado todo lo anterior podemos formalizar el concepto de delito informático como: **comportamiento criminal que se vale de las computadoras y los sistemas de comunicación para ser ejecutado en las personas o en sus propiedades, ya sean físicas o intelectuales**.

*José Gabriel Réding Domínguez, Jesús Alejandro Flores Hernández; docentes de informática en la Dependencia Área Ciencias de la Información de la Universidad Autónoma del Carmen. Jorge Vázquez Torres, docente del Instituto Tecnológico Sur del Estado de Yucatán.

Los perjuicios de orden informático criminal contemplan las siguientes características:

•Trascienden todas las fronteras geográficas.
•No respetan condiciones sociales y/o económicas.
•Normalmente no son denunciados.
•Son efectuados por personas con conocimientos técnicos.
•Limitados por tiempo y espacio (realizados en fracciones de segundo y sin presencia física del autor).
•Son cometidos en, cada vez, un mayor número.
•Presentan atracción para individuos cada vez más jóvenes.
•Provocan pérdidas económicas o daños sociales.
•Ofrecen dificultad para su demostración.

Los requerimientos de integración y globalización informática, las transacciones de datos empleando las redes de cómputo y las telecomunicaciones dan pauta a la búsqueda de instrumentos que garanticen la integridad de la información y además provocan la generación de instrumentos que legalicen y aseguren la fiabilidad de las transacciones empleando medios de comunicación.

En algún lado se leía: *aún si la computadora estuviese apagada, en su caja y en un cuarto bajo llave, no estaría a salvo de ser accedida sin autorización*.

Para darnos una idea trascendental de la importancia de regular los delitos informáticos, debemos considerar tres aspectos acuñados para tal efecto: la acción engañosa, la provocación del error y por supuesto la disposición patrimonial (en el uso del sistema de cómputo y comunicaciones).

Para poder entender el concepto básico de delito, es menester definir al llamado sujeto activo, que en este caso, es aquella persona que posee los conocimientos especializados en computación y telecomunicaciones para poder llevar a cabo el delito, es más, podrían ser llamados criminales de cuello blanco, toda vez que distan del común denominador en materia de criminología. Por otro lado tenemos al llamado sujeto pasivo o víctima, mismo que puede o no tener conocimiento técnico de ordenadores o redes, pero que con el simple hecho de poseer una PC, estar conectado en la llamada Web o, inclusive, por tener información financiera, electoral, crediticia, de mercadeo, etc., en las bases de datos, lo hace candidato a ser atacado por los criminales informáticos.

Dado que el sujeto pasivo de un delito muchas de las veces no cuenta con el conocimiento técnico o el entendimiento suficiente en materia de cómputo, la mayoría de los daños informáticos no son descubiertos en tiempo o no son denunciados, lo que alienta al perpetrador a seguir con sus manipulaciones fraudulentas y provoca que las estadísticas conlleven cifras maquilladas o datos ocultos.

Autores como Julio Téllez Valdez consideran que los delitos informáticos pueden ser clasificados desde la óptica en que los sistemas de cómputo y comunicaciones son el "medio para llevarlos a cabo", o desde el "fin que persiguen estas actividades criminales". Dentro de la primera clasificación encontramos la falsificación de documentos, la manipulación de información confidencial, desviación de fondos, alteración en el funcionamiento de sistemas, acceso a áreas no autorizadas, intervención de medios o líneas de comunicación, etc.

Para el caso de la clasificación que considera el objetivo o fin, encontramos acciones como: bloqueos parciales o totales a los sistemas de cómputo y comunicaciones, destrucción y atentado en contra de los programas y del equipo en sí mismo, daño o retención no autorizada de medios magnéticos de almacenamiento, etc.

Una manera eficiente de prevenir los delitos de orden informático es promover la cultura de denuncia, divulgar las posibles y más comunes conductas de los criminales y su forma de contra restarlos. Lo anterior no es suficiente sin la debida legislación en los países que carecen de estos lineamientos. Basta con escuchar a algún conocido o ver las noticias para enterarse de que la información está lista para ser manipulada por personas malintencionadas.

Mucho se ha promulgado referente a las iniciativas que pretenden regular a los delitos informáticos, pero la realidad ha sido que en nuestro país y en muchos otros, la forma de hacer justicia, dista en gran parte de lo deseado por las organizaciones y por los individuos, toda vez que nuestro sistema de impartición se ve saturado por demandas de justicia y equidad, así como por recomendaciones, que en cada cambio de gobierno son olvidadas o ajustadas a intereses que no obedecen a la comunidad.

Las recomendaciones que hacen las instituciones letradas en este asunto, son encaminadas a la promulgación de normas que regulen la seguridad de los sistemas de cómputo y de comunicaciones, tanto hacia el exterior como al interior de las propias organizaciones. Desafortunadamente, el aspecto técnico, la divulgación del conocimiento y las leyes de transparencia, nos ponen en una encrucijada: dar a conocer todos los aspectos técnicos de los nuevos sistemas de cómputo y comunicaciones o permanecer indiferentes a las disposiciones de globalización y generación del nuevo conocimiento.

Tipos de Delitos Informáticos (según la ONU)

•Fraudes cometidos mediante la manipulación de computadoras: sustracción de datos, modificación de los programas, manipulación informática, fraude, otros.

•Falsificaciones Informáticas: alteraciones de documentos almacenados en las computadoras, modificación de documentos de uso comercial, etc.

•Daños o modificaciones de programas o datos computarizados. En este apartado se considera al llamado sabotaje informático el cual se realiza a base de virus, los gusanos, las bombas lógicas o cronológicas, otros.

•Accesos no autorizados a servicios y sistemas informáticos. En este rubro aparece el llamado pirata informático (hacker), la reproducción no autorizada de programas informáticos de protección legal, otros.

Una postura muy particular, y a forma de conclusión, es considerar a los sistemas de cómputo como cien por ciento abiertos, es decir, sin limitantes técnicas para su entendimiento técnico o comprensión de funcionamiento e intercomunicación. Podemos suponer sistemas que no ofrezcan nada que explotar "negativamente", es decir, que no posean puertos o rutinas que ocasionen intromisiones no autorizadas; pero la verdad esto es una idea sumamente filosófica, ya que siempre tendremos la amenaza de individuos "inconformes con el sistema" que buscan, a través de sus acciones ser redimidos.

Bibliografía

·Téllez Valdés, Julio. *Derecho Informático*. Mc Graw Hill
·*Ley de Vías Generales de Comunicación*. Colección Porrúa. México
·Internet.Instituto de Investigaciones Jurídicas UNAM
·Schwartz, Mischa.*Transmisión de Información, Modulación y Ruido*.Mc Graw Hill