ASPECTOS GENERALES DE LOS DELITOS INFORMÁTICOS Y EL COMBATE A LOS MISMOS

Autor: Pedro Torres-Ruiz

Introducción

En la actualidad, es indispensable utilizar en cualquier ámbito laboral los ordenadores para poder obtener, intercambiar y visualizar información que requiera el individuo. Esto ha sido posible gracias a la tecnología (hecha por el hombre), la cual ha contribuido a simplificar el trabajo. Sin embargo, no hay que olvidar que, cualquier alteración, modificación y/o uso indebido de la información, ya sea prensa escrita o Internet, es una violación a los derechos de autor.

El objetivo fundamental de este trabajo es analizar, explicar y sintetizar el origen de este problema desde el punto de vista informático, y una vez entendido, hablar en términos generales lo que compete al Derecho. Esto con el fin de proponer posibles soluciones en lo que se refiere al sujeto que comete el delito. Es importante destacar que las mismas autoridades competentes a nivel nacional y mundial han legislado sobre esta cuestión, pero no en forma satisfactoria, mediante convenios y tratados que se mencionarán más adelante.

No hay que olvidar tampoco que México ha hecho y continúa haciendo grandes esfuerzos por combatir este problema, y que a consecuencia de los actos terroristas que se ha vivido desde el comienzo del siglo XXI en distintas partes del mundo (Estados Unidos, España e Inglaterra) hasta el momento, como también en los medios electrónicos, el país se ha visto en la necesidad de reforzar no solamente su seguridad interna, sino también de participar activamente y en conjunto con varios países en la lucha contra el terrorismo en cualquiera de sus formas, real o virtual.

Definición de Conceptos

Es importante comenzar definiendo los conceptos de delito e informática, para luego discutir el término de delito informático y tener bien claro lo que se quiere decir:

1. Delito: Acción u omisión voluntaria o imprudente penada por la ley. [1]
2. Informática: Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento informático de la información por medio de ordenadores. [2]

Por su parte, el delito informático se explica como la acción voluntaria de un individuo capaz de obtener, almacenar, modificar, distribuir, intercambiar, utilizar y transmitir la información a través de ordenadores, ya sea por medio de dispositivos externos (impresoras, discos flexibles, discos compactos, entre otros), software e incluso firmware (un registro almacenado en la memoria de sólo lectura del ordenador) quebrantando la ley.

Tipos de delitos informáticos

En los países ricos se cuenta con leyes que hablan sobre los delitos informáticos, los cuales están sancionados por penas que van desde los seis meses hasta dos años de cárcel, y con una multa variada que en ocasiones no alcanza derecho a fianza. En algunos países con menores recursos, existen solamente unos cuantos apartados dentro de sus respectivas Constituciones, mientras que otros ni siquiera lo tienen contemplado como un delito.

Los delitos informáticos que se conocen están caracterizados de distintas maneras y he aquí algunos ejemplos:

[1] Diccionario de la Lengua Española. 22ª. Edición 2001, p. 743.

1. Acceso en forma abusiva a la información
2. Introducción y ejecución de virus informáticos
3. Intercepción abusiva
4. Espionaje y falsificación
5. Violencia sobre bienes informáticos
6. Abuso de la detentación y difusión de códigos de acceso
7. Violación de correspondencia electrónica
8. Ultraje de información
9. Pornografía

Esta serie de delitos va acompañada de un concepto llamado ingeniería social, el cual se refiere a una serie de mecanismos de captación de información con el fin de acceder a ordenadores y realizar las actividades ilícitas antes mencionadas, como por ejemplo: los malware (software maliciosos, del cual, surgen los virus y los spyware) los ataques a servidores, el phishing (falsificación de identidad), y el spam (correo no deseado), principalmente.

Es importante destacar que hasta hace poco tiempo, a través de la criptografía se podía clasificar mensajes de manera pública o privada, por ejemplo, mandar un mensaje a un destinatario para que, éste a su vez, lo pudiera encriptar y codificar a través de una clave que el mismo destinatario poseía, siempre y cuando esto se llevara a cabo bajo un diseño y canal de comunicación seguros tanto del navegador como del servidor del que se trate.[3] Sin embargo, en la actualidad, esto ya se volvió arcaico, debido a que los hackers y crackers han implementado nuevas formas más sofisticadas de sabotear los sistemas informáticos.

---

[2] Diccionario de la Lengua Española. 22ª. Edición 2001, p. 1275.
[3] Ver Pedro Torres-Ruiz, "Luces y Sombras del Internet en la Sociedad Mexicana," Tesis de licenciatura, Universidad del Valle de México, México, D.F. 2000.

En este nuevo contexto, es necesario definir y explicar claramente el papel de hacker y cracker. Esto es importante dada la confusión existente respecto a las actividades que cada uno de ellos realiza, siendo estigmatizados ambos como *“terroristas”* por la sociedad. Es fundamental también para entender el por qué de los delitos informáticos que se cometen a diario.

Primero, tenemos al hacker que es un individuo que se introduce y modifica los sistemas de información de cualquier empresa, institución nacional o extranjera e incluso de individuos, siendo una persona hábil que cuenta con un código de ética como son: difundir la información obtenida por él mismo pero sin obtener nada a cambio, no dañar algo de manera intencional, modificar el acceso y evitar ser identificado y sobretodo, realizar acciones en servidores ajenos para no ser rastreado de forma inmediata en puntos alámbricos e inalámbricos cercanos. Incluso, esta figura ha sido contratada por empresas de distintas ramas para salvaguardar los sistemas computacionales, combatiendo los virus y a los creadores de los mismos.

Por otro lado, el cracker se enfoca particularmente al diseño de virus informáticos que él mismo introduce con el fin de alterar información, esto sí, para fines propios y de manera intencional y sin ningún código de ética, como son: la defraudación, la burla, o el terrorismo entre otros. Otro actor que participa paralelamente con el cracker es el pirata informático, cuyo trabajo es la sustracción de información para la comercialización ilegal de copias de software legales con fines de lucro, adueñándose de los derechos de autor, así como el uso de técnicas para desproteger los programas y su utilización en forma ilegal.

Combate a los Delitos Informáticos a Nivel Nacional

Ahora bien, en materia de Derecho, existen dos sujetos importantes cuyos papeles son: activo y pasivo. El sujeto activo consiste en aquel individuo que tiene la capacidad para enfrentar cualquier reto de tipo tecnológico que se le

presente, contando con un coeficiente intelectual por arriba de la media y decidido a cumplir con sus metas. Estas características son claramente identificadas en el caso de los hackers y crackers. El sujeto pasivo se refiere a aquellos actores involucrados por el sujeto activo, como son: individuos, instituciones, y gobiernos que son atacados a través de diversos sistemas informáticos por medio de redes. En algunas ocasiones, el hecho de compartir información entre los sujetos pasivos resulta en una valiosa herramienta para detectar si son o no amenazados por un actor activo, sin que éste último se percate de que ha sido descubierto.

Cabe señalar que existen ocasiones en que un individuo no tiene la intencionalidad de dañar los sistemas informáticos (negligencia, descuido, o ignorancia) cuando se encuentra trabajando en el ordenador, siendo interceptado por autoridades competentes. En algunos casos, esto se puede dar debido a que sea manejado virtualmente por cualquiera de los dos sujetos activos mencionados anteriormente. En estas situaciones hay que tener cuidado de no fincar responsabilidades de inmediato al individuo que es descubierto “in fraganti” sin antes investigar si efectivamente el ordenador o sus periféricos (bienes informáticos) son o no utilizados por terceros a través de canales de red alambicas y/o inalámbricas.

Con frecuencia, particularmente en México, tanto los individuos como las empresas no denuncian estos actos ilícitos por varias razones, tales como: falta de leyes para su protección; en el caso de las empresas, la reputación que tuvieran ante la sociedad por el temor de ser cuestionados sobre su capacidad para enfrentar tales situaciones y generar una serie de pérdidas económicas considerables para su negocio; y la falta de creación, investigación, entendimiento y tratamiento de leyes para este problema por parte de los legisladores.

También hay que mencionar, lo que expertos en Derecho Jurídico-Penal comentan al respecto: “Se ha dicho que algunos casos de abusos relacionados

con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas". [4]

Es necesario reconocer que actualmente México cuenta con distintas leyes que hablan sobre el derecho informático y sobre los derechos de autor. Entre ellas tenemos la Ley Federal del Derecho de Autor, el capítulo IV titulado "De los programas de computación y las bases de datos" de los artículos 101 al 106, el título VIII "De los registros de derechos" capítulo I artículo 164 y el capítulo II "De las infracciones en materia de comercio" artículo 231 fracción V, los cuales se refieren a la protección de los programas de computación así como de las bases de datos, al préstamo de cualquier material previa autorización del o los autores del mismo, así como a las infracciones en las que se incurran por uso indebido con fines lucrativos directa o indirectamente. Se cuenta también con el Código Penal y Procedimientos Penales de Sinaloa en el título Décimo, capítulo V titulado "el delito informático", concretamente el artículo 217 que explica sobre la violación de la información en cualquiera de sus modalidades por parte del individuo; el Código Penal en materia de Fuero Común y Federal, en particular el artículo 40, el cual se manifiesta sobre el aseguramiento de los bienes cuando es cometido un delito en forma intencional pero que, aún así no contempla claramente un delito informático como tal, debido a que los instrumentos para sustraer la información no son elementos suficientes para ser penalizados ya que si son datos, se esta hablando de algo intangible. Y finalmente la Constitución Política de los Estados Unidos Mexicanos, que en sus artículos 6º y 7º se hace mención sobre la regulación de la libertad de expresión y el derecho a la información,

[4] Estrada Garavilla, Miguel. Delitos Informáticas www.unifr.ch/derechopenal/articulos.htm#E

incluyendo el concepto de difamación. Sin embargo, ninguna de las leyes o tratados mencionados se refiere al sujeto que comete tal ilícito, ni al castigo y/o pena que se le debe aplicar por incurrir en tal delito.

Por otro lado, la Ley Federal de Telecomunicaciones publicó con fecha del 7 de junio de 1995 en el Diario Oficial de la Federación la definición de Internet; uno de varios medios de comunicación como el servicio que presta un usuario de la Red concesionada o pública de Telecomunicaciones, cuya actividad tiene efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida. Esto como referencia a que el Internet, también es un canal de información que, en la actualidad es el medio más común a ser utilizado para cometer delitos informáticos de cualquier naturaleza.

Combate a los Delitos Informáticos a Nivel Internacional

La firma del Tratado de Libre Comercio entre México, Estados Unidos de América, y Canadá en 1994, resultó en fuertes presiones para la homogeneización de las leyes en el área tecnológica y la regulación del Internet. Tanto los Estados Unidos como otros países de Europa cuentan con leyes que penalizan los delitos informáticos (Ver Cuadro No. 1).

Cuadro No. 1, Leyes Contra los Delitos Informáticos

Países	**Leyes o Tratados**
Alemania	Ley contra la criminalidad económica Creada el 15 de mayo de 1986

Francia	Ley sobre Fraude Informático No. 88-19 Creada el 5 de enero de 1988
Estados Unidos de Norteamérica	Acta de Fraude y Abuso Constitucional (1986) pero modificada por Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) en 1994
Austria	Ley de Reforma del Código Penal, creada el 22 de diciembre de 1987

Del 18 al 25 de abril del presente año se celebró el 11º Congreso de las Naciones Unidas sobre “Prevención del delito y justicia penal” en Bangkok, Tailandia, con el subtema “Sinergias y respuestas: alianzas estratégicas en materia del delito y justicia penal”. De especial importancia es el documento No. A/Conf. 203/14 titulado: *“Workshop paper 6: Measures to combat computer-related crime”,* presentado el día 19 de abril, donde un representante de Camerún comentó que debido a falta de legislación internacional sobre el combate al delito informático en el mundo aún se está lejos de erradicar tal problema. Para el 22 de abril, el comité número 2, encargado de discutir en el seminario 6 sobre las “medidas para combatir los delitos informáticos”, discutió sobre las recomendaciones que deben tomar gran parte de los países de los cinco continentes para el combate contra el delito informático, las cuales se presentan a continuación:

1. La creación de una cultura de seguridad en la navegación de Internet, -como una tecnología de información más utilizada en el mundo-. Más allá de la aplicación del derecho penal y sus leyes, es necesaria la aplicación de estrategias para la detección y combate hacia los usuarios activos con el fin de cumplir dos objetivos fundamentales: el funcionamiento seguro para generar confianza óptima en los negocios y

de esa manera tener una economía que se fortalezca; y tratar de solucionar las necesidades que cada país requiere en cuanto a la seguridad informática se refiere, ya sean pobres o ricos, pero en especial para los primeros, por su alta vulnerabilidad en el uso de esta tecnología de la información.

2. La necesidad de que el Sistema de Naciones Unidas juegue un papel preponderante mediante convenios o tratados internacionales, para asegurar el correcto funcionamiento y protección del Internet, y protegerse de los actores activos en lo que se refiere a infraestructura, desarrollo sostenible, protección al usuario, comercio electrónico, y transacciones bancarias.
3. La renovación en cada uno de los países participantes de sus leyes internas para el combate a los delitos informáticos, como son: el acceso ilegal a las redes de ordenadores, el ataque a las vías de comunicación, la destrucción de información, entre muchos otros temas destacados en los acuerdos sobre la materia en Europa.
4. La necesidad de que tanto los gobiernos, las empresas, y los organismos no gubernamentales trabajen en conjunto para, a través de instituciones educativas, capacitar a los profesionales de la justicia como son los jueces, abogados, y magistrados, a través de planes de estudio que incluyan el tema del crimen cibernético.
5. La necesidad de que el 11º Congreso sirva para incrementar la atención a establecer, mejorar, y ampliar las herramientas básicas actuales para el intercambio de información, detección y mecanismos de respuesta, así como las medidas en la lucha contra el crimen cibernético. Para ello, debe inspirarse en las actividades llevadas a cabo por la INTERPOL, las cuales se han visto reflejadas en la convención “Cybercrime” del grupo de los ocho, en donde se discutió sobre los mecanismos de alerta de los equipos que dan respuesta a la emergencia de un ordenador (CERTs),

y del foro de los equipos de la respuesta y de la seguridad del incidente (PRIMEROS), los cuales todavía se limitan a algunos países europeos y a los Estados Unidos. Estas herramientas también deben de estar disponibles internacionalmente para compartir los conocimientos y la información referente a los medios de reconocer, prevenir, y responder a los nuevos tipos (A/CONF.203/1422) de delitos cibernéticos e informar al público los mecanismos eficaces de respuesta. Se debe poner especial énfasis en estas herramientas prácticas y ponerlas a disposición de los países en vías de desarrollo ofreciendo el entrenamiento requerido.

6. En lo que se refiere a la política de evaluación del crimen cibernético, esta se debe basar en un esquema de eficacia y eficiencia, pero siempre y cuando, todos los países participantes a nivel internacional establezcan mecanismos de financiamiento, estén coordinados para llevar a cabo tal investigación práctica, y estén conscientes de que cada día surgen nuevos delitos informáticos.
7. Finalmente, se anunció que la oficina de las Naciones Unidas para el combate a las Drogas y el Crimen (UNODC) presentaría, para su consideración, las medidas para el combate contra el crimen cibernético en la segunda fase del congreso de la Sociedad de la Información celebrada en Túnez de este año.

Impacto de la Informática en el Ámbito Político a Nivel Nacional

Las elecciones federales que se realizaron en México en el año 1997 fueron confiables, en gran medida, debido a la creación de una Comisión de Informática dependiente de la Unidad Técnica de Servicios de Informática del Instituto Federal Electoral (IFE), la cual puso en marcha un Programa de Resultados Electorales Preliminares (PREP), siendo todo un éxito para las elecciones de 1997, 2000 y 2003. A su vez, esto contribuyó a que se le diera la

confianza al IFE en su conjunto. Pero en contraste con otros países como Australia, Canadá, Estados Unidos, Gran Bretaña, por mencionar sólo algunos, cuyas elecciones han sido realizadas con dispositivos electrónicos mediante distritos -no por votos como se hace en este país- y cuyos resultados son generados en unas cuantas horas por la alta confiabilidad, seguridad, y transparencia en los sistemas informáticos (a pesar de que también son vulnerables a cualquier ataque cibernético), esto no ha sido posible en México. Quizás esto se deba a que México aún no cuente con una infraestructura sólida, la cual se explica por diversos factores, como son: la desconfianza de los ciudadanos hacia las autoridades electorales, la falta de capacitación para operar estos dispositivos, y sobre todo, la inexistencia de una ley que regule estos aparatos electrónicos para evitar cualquier alteración, caída y/o fraude del sistema, a pesar de que ya se cuentan con aparatos electrónicos diseñados y fabricados por diversas universidades mexicanas y empresas con residencia en el país.

Los retos en esta área se incrementarán en el futuro, como resultado de algunas medidas tomadas recientemente. El 30 de junio del presente año, por ejemplo, el gobierno federal firmó un decreto sobre las adiciones y reformas en distintos puntos del Código Federal de Instituciones y Procedimientos Electorales, el cual permitirá a los mexicanos residentes en el extranjero votar por correo postal. Igualmente, en agosto de este año, autoridades electorales inauguraron el Centro de Cómputo y Resguardo Documental en Pachuca, Hidalgo con un costo de 37 millones de pesos en su construcción y que permitirá proteger las bases de datos de más de 230 millones de documentos electorales que tiene el Registro Federal de Electores (RFE) y que permitirá, entre otras cosas, confrontar datos e imágenes de los ciudadanos, así como la digitalización de la documentación de los mismos en vez de ser traslados de un lugar a otro y, crear una bases de datos secundaria dependiente de la primera para protección de la misma y como respaldo. En un futuro no muy

lejano, se tiene también contemplada la construcción de un centro de impresión para la emisión de credenciales de elector, impresión del padrón, y listas nominales.

La capacidad de las autoridades mexicanas para responder a los retos en esta materia será puesta a prueba el próximo año, cuando se efectuarán las elecciones federales, en las que el Instituto Federal Electoral será el encargado de coordinar y vigilar el proceso electoral. Dicho proceso electoral es crucial para los mexicanos, dada su importancia para facilitar el cambio de poder de manera democrática que cada seis años requiere el país. El país tendrá que continuar perfeccionando este proceso y responder de manera eficaz, imparcial, y transparente a los acuerdos firmados este año, antes mencionados.

Conclusiones

Es evidente que en México, todavía existe un vacío legal en cuanto a la regulación del uso de la información a través de distintos medios de comunicación. A pesar de que el gobierno federal en conjunto con los gobiernos locales y municipales del país han luchado contra la piratería de software y monitoreado y embestido contra la pedofilia, la pornografía infantil, así como el uso indebido de la información para distintos fines a través de la policía cibernética; aún persisten las actividades ilícitas, causando pérdidas anuales de millones de dólares para las empresas diseñadoras y proveedoras de software. El uso ilegítimo de sus productos contribuye a que no exista un desarrollo tecnológico sustentable en México, el cual permita competir con otras naciones.

Los delitos cibernéticos no se pueden erradicar de un día para otro, pero si es posible y urgente legislar y aplicar la ley para el combate a estos delitos con más rigor, pues aunque las autoridades competentes pongan a disposición de un Ministerio Público a estas bandas delictivas o actores individuales,

lamentablemente no se tienen elementos suficientes para fincarles responsabilidades por la falta de claridad en las leyes.

Finalmente, cabe mencionar que en noviembre del presente año, la empresa consultora GSP Global lanzará al mercado el estándar ISO 27001 que consistirá en la medición de seguridad informática tanto para software, ordenadores y redes de comunicación de las empresas, garantizando la protección de información del mismo. El costo de dicho estándar es alto, sin embargo, existen dos opciones para su adquisición: la primera opción es, contratar los servicios de una consultoría sin incluir equipo y software que va de los trescientos a seiscientos mil dólares, y la segunda opción es capacitar a los especialistas de la empresa para llevar a cabo la implantación del estándar, con un costo inferior a los doscientos mil dólares, según directivos de la empresa.

Propuestas

1. Reducir significativamente el costo de los programas informáticos en el mercado o en su caso, lanzar promocionales para su fácil obtención por parte de los usuarios finales y/o empresas con el fin de evitar que, estos últimos, recurran a lo que se le llama comúnmente *“mercado negro”* para la obtención del mismo de forma ilegal y sin garantías de que el producto funcione al cien por ciento.
2. Debido al desconocimiento de los términos informáticos por parte de los legisladores, es necesario, convocar y hacer participar a expertos en el tema en las comisiones que se creen para analizar, discutir y proponer soluciones para la regulación de los sistemas informáticos.
3. Legislar y actuar de manera correcta sobre aquellos individuos que cometan delitos informáticos en cualquiera de sus modalidades. Definir de manera clara el papel de los actores activos y de ser necesario,

proteger a aquellos cuya intención es trabajar de manera legítima por y para las entidades gubernamentales y/o empresas públicas o privadas en el uso de los sistemas informáticos. Concretamente, que en el Código Penal Federal se hagan modificaciones en los artículos referentes al delito informático, con el fin de definir al personaje o los personajes que cometen tal ilícito.

4. Establecer una serie de medidas preventivas para no caer en actos ilícitos que con frecuencia se cometen involuntariamente. Esto, mediante cursos, talleres, seminarios y/o congresos convocados por entidades gubernamentales, empresas y/o consultores independientes dedicados a este tema, enfocados para el público en general y/o a ciertos sectores.
5. Generar un clima de confianza tanto en las autoridades legislativas como electorales, principalmente en la correcta regulación de las leyes en materia de Telecomunicaciones e Informática, y la implantación de un sistema electoral computarizado confiable.