INVESTIGACION DEL DELITO INFORMATICO

Álvaro Villa T.

Resumen

Las sociedades modernas se caracterizan por un gran componente tecnológico-informático, lo que ha llevado consigo a la administración, análisis y accesos masivos a sistemas automatizados de información. Estos se encuentran presentes en ámbitos tales como gobierno, salud, sistema financiero, entre otros, es precisamente por este desarrollo informático donde se ha presentado un nuevo fenómeno delictivo el que en términos generales se le ha denominado delito informático, el cual se caracteriza principalmente por su forma de comisión, que es por medio de computadoras o bien se realiza a través de los sistemas automatizados de la información. Frente a ello se ha originado la informática forense, como una disciplina que permite abordar de mejor manera la investigación de esta clase de ilícitos, que ha llevado incluso a la creación de unidades especializadas en el esclarecimiento de este delito por parte de la policía y demás organismos encarrgados de la investigación criminal.

Abstract

Palabras claves: investigación delitos informáticos, delitos cometidos por medio de ordenadores, informática forense, sistemas automatizados de información.

Keywords

Introducción

En la actualidad es usual que los diferentes medios de comunicación (escritos, digitales, radiales, etc.) den cuenta de titulares como: "Detienen a autor del mayor caso de hackeo militar de la historia" [1], "cincuenta detenidos en la primera operación de Europa contra la piratería de señal de TV"[2], "¡cuidado con los "hackers!"[3], "Hackers diseñan nuevos métodos de ataque"[4], "los datos de 120.000 usuarios españoles, en manos de

[1] Sitio Web del diario La Tercera, [http://www.tercera.cl/medio/articulo/0,0,3255_5726_140396678,00.html, consultado el 10 de octubre de 2007].
[2] Sitio Web elmundo.es, [http://elmundo.es/elmundo/2007/05/30...180515414.html, consultado el 10 de octubre del presente año].
[3] Sitio web de la BBC, [http://news.bbc.co.uk/hi/spanish/science/newsid_4865000/4865348.stm, consultado el 10 de octubre de 2007].
[4] Sitio web terra.com, [http://www.TERRA.COM./NOTICIAS/ARTICULO/HTML/ACT987345.HTM, consultado el 10 de octubre de 2007].

"ciberpiratas"[5], "en dos años, las estafas informáticas les costaron a los estadounidense 7 mil millones de dólares"[6].
El que la prensa acapare en portada estos titulares obedece a una realidad que caracteriza a las sociedades de hoy, y que es precisamente que son de un marcado carácter tecnológico, donde el uso de la Internet aparece como una herramienta indispensable del diario vivir.
El avance de la ciencia y tecnología ha llevado consigo la aparición de un nuevo fenómeno delictivo del que hace 60 años no se tenía conocimiento, este es, el llamado delito informático, cibercrime, delito telemático, delito cometidos por medio de computadoras, son otras de las denominaciones que ha recibido.
En la doctrina no hay un consenso respecto de la definición de este fenómeno delictual, para algunos presenta una identidad propia y que además tutela un nuevo bien jurídico, cual es la información, en cuanto si misma, para otros por el contrario sólo obedece a ilícitos propios del mundo actual y que en general ataca bienes jurídicos conocidos, como la propiedad, la fe pública, entre otros, siendo su elemento diferenciador el especial medio de comisión, que usualmente será un computador o un soporte tecnológico como por ejemplo un teléfono móvil, PDAs (conocidas como PALM), o a través de los sistemas automatizados de información.
Este tipo de delito presenta características que lo hacen desde el punto de vista de su investigación muy difícil para su detección, dado que en la mayoría de los casos es complejo la conservación de los datos, en otras es imposible la identificación del sujeto activo a eso debe agregarse que muchas veces posee conocimientos relevantes sobre la materia, lo que de una o otra manera lo profesionaliza en esta clase de ilícitos,
Frente a este escenario las policías, el Ministerio Público y en general los organismos dedicados a la investigación han tenido que avanzar en ello y profesionalizarse, de esta manera se han creado en muchos países unidades especializadas para la investigación de estos delitos, las que han logrado establecer ciertos métodos de investigación que han permitido en algunas ocasiones esclarecer el delito e identificar a los autores o participes del mismo.

En el presente trabajo se expondrán algunos de los elementos más relevantes de la investigación forense del llamado delito informático.

1. Acerca del concepto de delito informático

Como se señaló la doctrina no está uniforme en una categoría propia e independiente de esta clase de delitos, de esta manera en términos generales se la de definido como "toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya omisión intervienen

[5] Sitio web diario El País, [http://www.elpais.com/articulo/espana/datos/120000/usuarios/espanoles/manos/ciberpiratas/elpepunac/20070611elpepinac_11/Tes, consultado el 10 de octubre de 2007].

[6] Sitio web diario Clarín, [http://www.clarin.com/diario/2007/08/14/um/m-01477990.htm, consultado el 10 de octubre del presente año].

dispositivos habitualmente utilizados en las actividades informáticas"[7], el profesor Klaus Tiedemann los ha definido como aquellos "actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos"[8], ambos conceptos son bastante amplios, por lo que restringiendo los conceptos se podría señalar que son aquellos en que el "ordenador representa el medio de ejecución".[9]
Se puede apreciar que la característica principal en estos delitos es la presencia del ordenador o computador como instrumento de comisión, pero, es necesario realizar una distinción ya que en algunos casos "el ordenador y sus aplicaciones constituyen el objeto material del delito (sobre el que recae físicamente la acción) y en otras será un mero instrumento para cometer hechos generalmente tipificados en el Código Penal"[10], segundo con esa línea las Naciones Unidas, en su oficina contra la Droga y el delito, ha señalado que la conducta en desplegada en la comisión del delito "implica la utilización de tecnologías digitales (...)se dirige a las propias tecnologías de la computación y las comunicaciones ; o incluye la utilización incidental de computadoras en la comisión de otros delitos".[11]

2. Características de la delincuencia informática

- Carácter transterritorial.
- La conductas no se realizan en un solo acto..
- Impunidad del sujeto activo por la utilización de Internet.
- Posibilidad en la eliminación de evidencias.
- Se les califica como delitos de cuello blanco

A continuación se referirá a alguna de ellas

2.1 Carácter transterritorial

Esta dado básicamente porque la acción y el efecto del delito no necesariamente se dan en un mismo espacio determinado, es más puede incluso estar separado por miles de kilómetros, ubicarse en continentes distintos, etc. y esto es así ya que el espació donde se desarrolla el delito no es físico si no virtual, donde por medio de la red puede accederse a cualquier rincón del mundo.
Esto trae no sólo trae como consecuencias lógica la legislación aplicable en el caso concreto si no además que puede "suceder que los distintos ordenamientos jurídicos posiblemente aplicables no coincidan en identificar la ilicitud de esa conducta".[12]

---

[7] Definición adoptada en las conclusiones del congreso sobre "Delito Informático", celebrado en Zaragoza, España, en 1989. En: MATA Y MARTÍN, Ricardo. *Delincuencia informática y derecho penal*, Madrid: Edisofer s.l., 2001, p.21.
[8] TIEDEMANN, Klaus. *Poder económico y delito*. Barcelona: Ariel, 1985, p. 122.
[9] MATA Y MARTÍN, Ricardo. *Delincuencia informática y derecho penal*, Madrid: Edisofer s.l., 2001, p.22.

[10] MATA, Delincuencia, p. 23.
[11] NACIONES UNIDAS, Oficina contra la Droga y el Delito. Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, [http://www.11uncongress.org, consultado el 11 de octubre de 2007].
[12] ÁLVAREZ, VIZCAYA, Maite. Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red. En: *Internet y derecho penal*. Director: LÓPEZ, ORTEGA, Juan. Madrid: Consejo General del Poder Judicial, cuadernos de derecho judicial, 2001, p.266

2.2 Impunidad del sujeto activo por la utilización de Internet.

En Internet existe la identidad digital que es el "conjunto de características propias de un individuo o de un colectivo en un medio de transmisión digital. (...) donde en un proceso de comunicación lo único que recibe una entidad- colectiva o individual- de otra son Bytes (...) los que son procesados por las aplicaciones correspondientes y presentados en el formato requerido (pantalla, sonidos...)".[13], esta identidad se debe crear y vincular a un individuo o un colectivo determinado.
Es precisamente gracias a que esta identidad digital puede crearse, en principio "nadie sabe quien esta al otro lado" [14], de esta forma un sujeto puede inventar "una personalidad virtual", que poco o nada tiene que ver con su identidad real, lo que lógicamente le facilita la comisión del hecho delictivo".[15]

3. El sujeto activo en el delito informático

Este presenta algunas peculiaridades que a continuación se detallan:

- Posen importantes conocimientos de informática.
- Ocupan lugares estratégicos en su trabajo.
- Sus edades fluctúan entre los 18 y 35 años de edad.

4. Principales figuras de delito informático

Las actividades ilícitas más recurrentes en contra de los sistemas de información se pueden encuadrar en cuatro grupos[16].

4.1. Interrupción

Es un ataque contra la disponibilidad, impide el uso normal o la gestión de los recursos informáticos y de las comunicaciones. Entre estos ataques se encuentran la denegación de servicio, por ejemplo el servicio de un servidor de correo.

Conductas relativas a que se enmarcan dentro del grupo interrupción

4.1.1 Sabotaje informático

[13] VILLÉN, SOTOMAYOR, Marta. La red y su evolución y utilización para actividades ilícitas. En: *Delitos contra y a través de las nuevos tecnologías. ¿Cómo reducir su impunidad?*. Director:: VELASCO, Eloy. Madrid: Consejo General del Poder Judicial, cuadernos de derecho judicial, 2001, p.42

[14] VILLÉN, "La red", p.42.

[15] ÁLVAREZ, "Internet", p. 267.

[16] La división en estos grupos es planteada por: PIQUERES CASTELLOTE, Francisco. *Conocimientos básicos en Internet y utilización para actividades ilícitas*. En: Cuadernos de derecho judicial, nº. 3, 2006, pp. 41-90, p.60.

"Toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes o componentes, su funcionamiento o de los datos contenidos en él"[17]. Dentro de esta clase se encuentran las siguientes técnicas:

4.1.2 Crash Programs o programas de destrucción progresiva

Son rutinas construidas dentro de programas de aplicación o dentro del sistema operativo, que permiten borrar un gran volumen de datos en un breve período.

4.1.3 Tome bombs, logics bombs o bombas lógicas de actuación retardada:

Estos programas persiguen la destrucción o modificación de datos en un momento futuro determinado.

4.1.4 Cáncer routine o rutinas cáncer: es una variación de las bombas lógicas:

Consiste en instrucciones que consumen en poco tiempo un software debido a que se expanden al autoreproducir el programa cáncer en distintas partes del programa de aplicación, escogidas aleatoriamente, durante cada uso.

4.1.5 System crash:

Programas que logran un bloqueo total del sistema informático afectando el sistema operativo y los programas almacenados, colapsando el disco duro.

4.1.6 Programas virus

Programa computacional que puede producir alteraciones más o menos graves en los sistemas de tratamiento de información a los que ataca.

4.2 Interceptación

Es una entidad no autorizada que consigue acceso a un recurso o a un sistema automatizado de datos. Es un ataque contra la confidencialidad. La entidad no autorizada puede ser una persona, un programa o un ordenador. Dentro de esta clase se encuentran las siguientes técnicas:

Conductas relativas a que se enmarcan dentro del grupo interceptación

4.2.1 Espionaje informático

"Consiste en la obtención no autorizada de datos almacenados en un fichero automatizado, en virtud de lo cual se produce violación de la reserva o secreto de información de un sistema de tratamiento de la misma"[18]. Dentro de las formas de comisión del espionaje, los de mayor frecuencia son:

[17] HUERTA, MIRANDA, Marcelo. *"Figuras delictivo-informáticos tipificadas en Chile"*. En Revista de derecho informático, alfa-redi, n° 20, marzo, 2000. [http://www.alfa-redi.org/rdi-articulo.shtml?x=433, consultado el 01 de junio de 2007].

[18] HERRERA BRAVO, Rodolfo. *Reflexiones sobre la delincuencia vinculada con la tecnología digital (basadas en la experiencia chilena)*. Asociación de Derecho e Informática de Chile, ADI. (http://www.adi.cl/b_docs_propios3.html, consultado el 12 de octubre de 2007).

4.2.2 Witetapping o pinchado de líneas

Consiste en una intercepción programada de las comunicaciones que circulan a través de las líneas telefónicas, con el objeto de procurarse ilegalmente la información, pero permitiendo a la vez la recepción normal de la transferencia de datos o comunicación, característica que lo hace difícilmente detectable.

4.2.3 Electronic Scavenging o recogida de información residual

Se lleva a cabo cuando una persona "obtiene información que ha sido abandonada sin ninguna protección como residuos de trabajo[19]" Generalmente se refiere aquella información que se encuentra en la memoria RAM del computador la que sólo se borra cuando se apaga el equipo.

4.2.4 Hacking directo

"Consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o password, no causando daños inmediatos y tangibles a la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor"[20].

4.2.5 Hacking indirecto

Es un acceso indebido a un sistema de tratamiento de la información con el objeto de cometer delitos, tales como, defraudaciones, sabotajes, falsificaciones, entre otros. Esta modalidad se presenta como un medio (informático) para la comisión de otros delitos.

4.3 Modificación

Por definición es una entidad no autorizada que logra acceder a un recurso y/o sistema automatizado y es capaz de manipularlo. Es un ataque contra la integridad; por ejemplo, la alteración de un programa (soporte lógico) para que actúe diferente.

Conductas que se encuadran dentro del grupo Modificación

4.3.1 Fraude informático

Es "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en

[19] HUERTA M, "Figuras", p.21.

[20] LÍBANO MANZÚR, Claudio. *Los delitos de Hacking en sus diversas manifestaciones.* Revista de derecho informático, alfa-redi, n° 021, abril, 2000. (http://www.alfa-redi.org/rdi-articulo.shtml?x=433, consultado el 20 de abril de 2007).

cualquiera de la fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de terceros"[21].

Estas manipulaciones pueden darse tanto en el ingreso y salida de datos al sistema de información.

4.3.2 Manipulaciones en el input o entrada de datos (data didling)

"Los datos son capturados en documentos originales, tales como registros o facturas, y mediante un método se pueden introducir a la máquina para su proceso. En esta fase se produce la generalidad de los fraudes informáticos , a través de la introducción de datos falsos al ordenador con el objeto de defraudar" .[22]

4.3.3 Manipulaciones en los programas

Con ellas "es posible que datos verdaderos que han entrado correctamente, sean alterados en su tratamiento arrojando resultados falsos, gracias a la modificación, eliminación o agregación de algunos pasos del programa".[23]
Las técnicas más usadas en este sentido son:

- Superzapping o llave maestra: "Es un programa de acceso universal y es un herramienta imprescindible en instalaciones de cierta dimensión cuando fallan los procedimientos normales para recuperar o reiniciar el sistema, ya que permite entrar en cualquier punto de éste en caso de averías u otras anormalidades".[24] Su mal uso permite alterar, borrar, copiar, etc. de cualquier forma no permitida los datos almacenados en el computador, sin que quede constancia de ello.
- Caballo de roya (trojan horse): "Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto".[25]
- Técnica salami o rounding down: "Consiste en introducir o modificar ciertas instrucciones de ejecución en un programa con el objetivo de extraer de determinadas cuentas pequeñas cantidades de dinero nominal, transfiriéndolas automáticamente a una cuenta corriente que ha contratado el sujeto activo".[26]

4.3.4 El Phishinh

Consiste en "suplantar la página web de una entidad de crédito, fundamentalmente, pero también de cualquier otra empresa de la que se pueda obtener beneficio económico, haciendo creer al usuarios que se encuentra ante la página oficial de la

[21] ROMEO, *Poder Informático,* p. 47.
[22] HUERTA M, "Figuras", p.16.
[23] HUERTA M, "Figuras", p.17.

[24] HUERTA M, "Figuras", p.17.

[25] HUERTA M, "Figuras", p.18.

[26] HUERTA M, "Figuras", p.18.

misma. Con ello se consigue obtener la información personal y las claves de los usuarios para con ellas poder realizar transacciones no consentidas por estos".[27] Para su realización no se requieren mayores elementos fuera de la capacidad para hacerlo, basta un computador y una conexión a Internet.

4.4 Reproducción no autorizada de programas informáticos

Básicamente se refiere a la piratería la que consiste en la distribución o reproducción ilegal de las fuentes o aplicaciones de software (programas) para su utilización comercial o particular.

5. Acerca de la informática forense

Frente a las diversas formas de ataques de los llamados delitos informáticos nace la informática forense como aquella disciplina que "que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia" [28](tribunales o juzgados).

6. Objetiva principal de la informática forense

Atendida la dinámica y naturaleza de esta clase de delitos, el perito informático tiene como función principal la de "recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal"[29]

Evidencia digital y material

La informática trabaja en dos escenarios sobre los cuales realizará el perito sus respectivos análisis, uno de ellos es el hardware (evidencia material) que se refiere a los componentes físicos de un sistema informático en particular tales como el monitor o pantalla, impresora, módems, reuters, entre otros y el otro se refiere al componente lógico es decir, a los

[27] FERNÁNDEZ LÁZARO, Fernando. La red y su evolución y utilización para actividades ilícitas. En: *Delitos contra y a través de las nuevos tecnologías. ¿Cómo reducir su impunidad?*. Director:: VELASCO, Eloy. Madrid: Consejo General del Poder Judicial, cuadernos de derecho judicial, 2001, p134

[28] ACURIO DEL PINO, Santiago. "Introducción a la informática forense". Revista de derecho informático, alfa-redi, n° 110, septiembre, 2007. (http://www.alfa-redi.org/rdi-articulo.shtml?x=9608 , consultado el 11 de octubre de 2007).

[29] ACURIO S, "Introducción", p. 8.

programas computacionales, esto es, un conjunto de instrucciones para ser usadas por el ordenador con el objeto de obtener un determinado proceso o resultado.