

# El Cibercrimen

Lic. Aldo R. Valdez Alvarado  
 Universidad Mayor De San Andrés  
 Carrera De Informática  
 Simulación de Sistemas  
[aldo\\_valdez@hotmail.com](mailto:aldo_valdez@hotmail.com)

## RESUMEN

En el presente artículo se da una visión general, desde la tipificación de los delitos informáticos, hasta como se define el Cibercrimen y las diferentes categorías que se tienen.

## Palabras Clave

Delito informático, seguridad, derecho penal, vulnerabilidad, confidencialidad, privacidad, cibercrimen.

## 1. INTRODUCCIÓN

Hoy en día, vivimos y trabajamos en un mundo de conectividad global, es decir, podemos tener una conversación casual, o podemos realizar una transacción multimillonaria con alguna persona al otro lado del planeta, de manera rápida y barata. Es que hoy en día se puede encontrar PC's a un costo antes inimaginado, también tiene que ver el abaratamiento de las tarifas de Internet y la proliferación de nuevas tecnologías de telecomunicaciones, que hacen que se cambie la forma en que pasamos nuestro tiempo de ocio o realizamos negocios

En relación con lo anterior podemos decir que la forma con que se realizan los crímenes también a cambiado, desde la aparición a mediados de los 90 de la novela "The Hacker Crackdown" hasta los últimos ataques a corporaciones millonarias como Microsoft, muchos de los procedimientos descritos en la primera y utilizados en la segunda se han mejorado y han experimentado crecimientos exponenciales y ahora vivimos rodeados de lo que se ha estado denominando como "Cibercrimen".

## 2. DELITO INFORMÁTICO

Cuando se producen siniestros hechos dolosos e ilícitos que vulneren la seguridad y confidencialidad de un sistema informático, se piensa primero en las TIC's (Tecnologías de la Información y la Comunicación) como una variable, que exponencialmente y progresivamente, se encuentra cada vez más presentes en la comisión de delitos.

La tecnología computacional, los archivos y documentos electrónicos, las bases de datos, los discos duros, los correos electrónicos y la red Internet son herramientas esenciales de una empresa o de un servicio público, cuyo mal uso o uso ilícito a través de soportes computacionales y violando su confidencialidad o reserva debe sancionarse penalmente o

mediante la tipificación de delitos informáticos..

### 2.1. Definición y Objeto del Delito Informático

En la formulación de esta definición se debe comprender todas las modalidades de ilícitos posibles. Por consiguiente una definición clásica de Delito Informático es aquella que la define como una conducta típica tipificada o establecida como ilícito por la ley, antijurídica (contraria al derecho) y culpable (con intención dolosa o por negligencia), cometida contra el soporte lógico de un sistema informático o de tratamiento automatizado de información (programas o instrucciones y datos de cierta naturaleza o importancia), generalmente mediante elementos computacionales.

Se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa un equipo informático, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con los ordenadores", "crímenes por ordenador", "delincuencia relacionada con el ordenador".

Sin embargo si revisamos la literatura y la normativa tanto nacional como internacional, se puede observar que no se tiene una definición ampliamente aceptada, sino más bien que se tienen diferentes acepciones en diferentes países, como en España donde se define el Delito Informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española".

De lo anterior podemos definir delito informático como: "son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal y que en su realización se valen de los ordenadores como medio o fin para su comisión".

En materia de criminalidad informática solo es necesario tipificar o crear nuevos delitos para castigar aquellas conductas que atenten contra el soporte lógico de un sistema, contra el software entendido en un sentido amplio, contra ciertos datos y/o documentos relevantes procesados y almacenados en un ordenador, es decir, que pueden ser manipulados, hurtados, destruidos, etc., y contra los programas o instrucciones que determinen el funcionamiento del mismo, los cuales pueden ser modificados, copiados ilegalmente y sin autorización, etc.

### 3. CIBERCRIMEN

#### 3.1. Introducción

Un escritor de ciencia ficción acuñó el término “ciberespacio” en 1983. El ciberespacio es el lugar en el que una conversación telefónica parece tener lugar, no en el interior del teléfono de tu casa o el de otra persona, sino más bien “el lugar entre” los teléfonos.

Sin embargo, estos últimos años, ya no se trata solo de “el lugar entre” teléfonos, sino también del uso que se le ha dado a la red telefónica, para la televisión primero y luego para la Internet.

Aunque no es exactamente “real”, el “ciberespacio” es un lugar que existe, donde ocurren cosas realmente reales. Este lugar no real, es muy importante, debido a que millones de personas han dedicado su vida a él, realizaron trabajo en él, se divertieron en él, e incluso se enamoraron y casaron en él, es más cada vez más personas escapan de su “realidad” hacia su “comunidad virtual”.

La vida humana, la verdadera vida, es imperfecta por naturaleza, y son humanos los que se encuentran en el ciberespacio, por lo que la forma en que vivimos en el ciberespacio es un reflejo de la forma en que vivimos en el mundo real, llevamos con nosotros nuestras virtudes y nuestros problemas. Entonces si en el mundo real existen delincuentes en el ciberespacio estos son ciberdelincuentes, y lo que realizan cibercrimen.

#### 3.2. Definición

Aunque parezca irónico, la palabra cibercrimen no se encuentra en ningún diccionario, ni siquiera es reconocido por el Word 2007 como una palabra que se encuentre en su diccionario, sin embargo una búsqueda en Google, nos muestra un sin número de páginas relacionadas a este término.

Al igual que en la definición de Delitos Informáticos no existe un común acuerdo sobre lo que es el cibercrimen. De manera general podemos definir el Cibercrimen como una subcategoría de los delitos informáticos. El término “cibercrimen” se refiere a crímenes realizados usando la Internet u otro tipo de redes de computadoras que se usan para cometer este crimen. Las computadoras y las redes se encuentran involucradas en estos crímenes debido a:

- La computadora o la red puede ser el arma del crimen, es decir, usada para cometer el crimen.
- La computadora o la red puede ser el objetivo del crimen, es decir, la “víctima”.
- La computadora o la red puede ser usada para propósitos incidentales relacionados al crimen, es decir, por ejemplo mantener registros de ventas ilegales de drogas.

Sin embargo existen otras definiciones que analizaremos a continuación debido a su importancia. El Departamento de Justicia de los Estados Unidos de Norteamérica define el cibercrimen como: “cualquier violación de la ley criminal que involucra el conocimiento de tecnología computacional, para su consumación, investigación o persecución”. Como se puede observar bajo la anterior definición, casi cualquier crimen podría considerarse como cibercrimen, por ejemplo, un detective que busca en una base de datos sospechosos de un delito.

El cibercrimen ha cruzado las fronteras estatales y nacionales de casi todos los países del mundo, entonces podemos tener una definición de una organización internacional. En el décimo congreso de la Naciones Unidas para la Prevención del Crimen y el trato de los Delincuentes, en el taller relacionado a los crímenes relacionados con las redes de computadoras, el cibercrimen se dividió en dos categorías y se definió como:

- a) El cibercrimen en sentido limitado puede ser cualquier comportamiento dirigido a operaciones electrónicas que tienen como blanco la seguridad de sistemas computacionales y los datos procesados por ellos
- b) El cibercrimen en sentido más amplio puede ser cualquier comportamiento ilegal cometido por, o en relación a, un sistema computacional o redes de computadoras, incluyendo crímenes tales como la posesión ilegal y ofreciendo o distribuyendo información a través de un sistema computacional o redes de computadoras.

Por supuesto como se puede observar estas definiciones son complicadas debido al hecho de que pueden ser ilegales en una nación pero no en otras.

La anterior definición se complementa con los siguientes ejemplos concretos:

- Acceso no autorizado.
- Daños a programas o datos computacionales.
- Sabotaje computacional.
- Intercepción no autorizada de las comunicaciones.
- Espionaje Computacional.

Estas definiciones aun no definitivas, pueden darnos un buen punto de partida para determinar lo que significa el término cibercrimen.

Por que es importante desarrollar una definición estándar de cibercrimen. A menos que todos usemos, o por lo menos substancialmente, definiciones similares, es imposible para el personal de IT, usuarios y víctimas, oficiales de policía, detectives, perseguidores y jueces discutir el delito inteligentemente. Por esa razón, también continuara siendo imposible recolectar estadísticas significativas que pueden ser usadas para analizar patrones y tendencias criminales.

### 3.3. Categorías de Cibercrimen

Es muy útil definir categorías de cibercrimen y entonces ubicar actos específicos dentro estas categorías. Primero, debemos entender que los cibercrimenes dependiendo de su naturaleza se pueden ubicar en categorías ya usadas para poder identificar diferentes tipos de crimen.

Existen muchas formas de categorizar el cibercrimen, para empezar podemos dividirlos en dos grandes categorías como son: cibercrimenes violentos o potencialmente violentos, y crimines no violentos.

#### 3.3.1. Cibercrimenes violentos o potencialmente violentos

Este tipo de crímenes usan redes de computadoras, tienen la prioridad mas alta por razones obvias. Estos crímenes pueden realizar daño físico a alguna persona o personas, los tipos de esta categoría incluyen:

- Ciberterrorismo.
- Amenazas de ataques.
- Ciberespionaje.
- Pornografía Infantil

#### 3.3.2. Cibercrimenes no violentos

La mayoría de los cibercrimenes son crímenes no violentos debido al hecho de que la principal característica de este mundo en línea es la capacidad de interactuar sin necesidad del contacto físico. El anonimato y lo irreal de estas experiencias virtuales son los elementos que hacen del ciberespacio un lugar tan atractivo para realizar crímenes. Los tipos de esta categoría incluyen:

- Ciberviolaciones.

- Ciberrobo.
- Ciberfraude.
- Cibercrimenes destructivos.
- Publicitar o solicitar servicios de prostitución en Internet.
- Apuestas por Internet.
- Venta de drogas por Internet.
- Lavado de dinero por Internet.
- Cibercontrabando.

### 4. CONCLUSIONES

El mundo del Cibercrimen y los delitos informáticos son mas bien un problema ético, de detección de las llamadas “vulnerabilidades” y de seguridad preventiva para el uso y el acceso. a los documentos almacenados en sistemas informáticos, que un asunto de tipificación legal de delitos idóneos.

### 5. REFERENCIAS

- [1] Bacard A. The Computer Privacy Handbook. 1995. Ed Peachpit Press. Barkeley.
- [2] Eckert W. Introduction to Forensic Sciences. 1997. Ed CRC Press. Nueva York.
- [3] Khoo M. Computer Forensics – Tracking the Cyber Vandals. 2002. Ed BlackHat Asia. Singapur.
- [4] Littlejohn D. Cybercrime Computer Forensics Handbook. 2002. Ed Syngress Publishing Inc.
- [5] Miller S. Civilizing Cyberspace. 1996. Ed. ACM Press. Nueva York.
- [6] Sterling B. The Hacker Crackdown. 1994.