LOS DELITOS ELECTRONICOS

Por: Gino Ríos Patio *

Resumen:

El presente artículo presenta, en general, una reflexión sobre la preocupante amenaza para la seguridad y tranquilidad de las personas naturales y jurídicas, que representa el notorio incremento y la aparición de nuevas modalidades de los delitos electrónicos; y en particular, explica en qué consisten dichos actos ilícitos y cuál es el nivel de lesividad que tienen.

Palabras Clave: Delito electrónico, Caballo de Troya, Salame, Delito de Cuello Blanco, Cifra negra de la Criminalidad, Criptografía digital.

Sumario:

INTRODUCCION

Con el tema del epígrafe, los Centros de Estudios de Criminología y de Derecho y Tecnología de la Facultad de Derecho de la Universidad de San Martín de Porres, organizaron recientemente un evento académico, en el cual el Jefe de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional, expuso la problemática actual que confronta nuestra sociedad frente a estas nuevas modalidades delictivas, las que fueron analizadas y comentadas por los Presidentes de los mencionados Centros.

En el referido evento quedó claro que el desarrollo cada vez mayor del comercio electrónico pone de manifiesto la necesidad de ejercer un control más estricto para salvaguardar los derechos e intereses legítimos de todos los que intervienen en dichas actividades comerciales.

De igual manera, ocurren otros actos que no son defraudatorios, pero sí son una amenaza a la seguridad y confianza que deben presidir las comunicaciones; así como a la intimidad y reputación de las personas.

El escenario de estos delitos es el ciberespacio, cuya naturaleza es virtual, esto es, existe solo aparentemente y no es real, siendo entonces lo contrario a actual, efectivo o real, sin embargo, puede producir un efecto, como son, para efectos del tema materia de este artículo, los delitos o fraudes que ocurren en él, que sí son reales, como cuantiosos los daños y perjuicios que se irroguen.

Esta especial circunstancia de la virtualidad coloca en indefensión legal a las víctimas, lo cual constituye un acicate para el delincuente, quien se ve atraído por el anonimato en el que actúa, lo que dificulta su identificación para fines investigativos y de sanción.

A lo anterior se debe adicionar el hecho de que las normas penales no prevén todas las conductas criminales que se realizan a través del espacio cibernético, existiendo por tanto vacíos legales que son aprovechados por los delincuentes informáticos, por tratarse de una actividad y un medio tecnológico que es muy dinámico en su desarrollo.

CONCEPTO

El delito electrónico, también denominado informático, es la conducta típica, antijurídica y culpable, no ética o no autorizada, vinculada al procesador automático de datos y/o transmisiones de datos.

Como se puede apreciar, es una delincuencia moderna, tecnológica, especializada, que por los instrumentos que utiliza, es capaz de extinguir toda huella de los actos.

Estos delitos utilizan la informática como objeto del ataque o como el medio para cometer otros delitos, frecuentemente de carácter patrimonial, como estafas, apropiaciones indebidas, etc. La tecnología informática es así una herramienta idónea por la gran cantidad de datos que acumula, por la increíble facilidad de acceso a ellos y la manipulación de esos datos.

Debemos tener conciencia que esta clase de ilícitos son devastadores debido a que permiten entregar datos e informaciones sobre millones de personas, naturales y jurídicas, inclusive el propio Estado, que son fundamentales para el funcionamiento de sus actividades de todo tipo.

En el evento, quedó planteada la pregunta de si era posible la creación de una plataforma tecnológica confiable regulada por un ordenamiento jurídico actualizable de acuerdo a sus necesidades.

CLASES DE DELITOS ELECTRÓNICOS

El expositor, experto investigador en esta clase de delitos, refirió que internacionalmente se conocen los siguientes delitos electrónicos:

1.- El "Caballo de Troya": consiste en introducir en un sistema conocido por el autor del delito y desconocido por la víctima, un programa informático a través del cual puede acceder a ese u otros programas del usuario.

2.- El "Salame": consiste en alterar un programa informático que maneja cuentas bancarias para que montos pequeños (centavos), se acrediten en otras cuentas manejadas por el autor, de las que luego extrae el dinero así obtenido.

3.- Falsificación informática: consiste en utilizar la computadora para falsificar documentos.

4.-Reproducción no autorizada de programas informativos de protección legal: consiste en afectar la propiedad intelectual.

5.-Daños al software: consiste en acceder al software, violar las defensas existentes y alterar o destruir los datos, a través de, por ejemplo, la "bomba lógica", que consiste en la alteración de un programa para detener el funcionamiento del sistema en el momento decidido por el autor del hecho, destruir los datos o los programas de los mismos; el virus informático, que consiste en insertar una instrucción en un programa que se transmite sucesivamente entre los diversos usuarios y causa el contagio entre los equipos informáticos, con la consecuente destrucción de todos o parte de los sistemas con los que opera al ingresarse una determinada instrucción o en un tiempo dado.

ASPECTOS CRIMINALISTICOS Y CRIMINOLOGICOS

Los delitos electrónicos pueden ser denominados o clasificados entre los delitos conocidos como “de cuello blanco”, por cuanto sus autores deben poseer ciertos conocimientos técnicos especializados para perpetrarlos en milésimas de segundo y no necesitan de presencia física; ello aunado a su sofisticación, hace que la cifra negra de esta criminalidad sea muy alta.

Dada la expansión cada vez más creciente de la tecnología informática y las facilidades para que los jóvenes la asimilen y practiquen, estos delitos tienen la tendencia a proliferar cada vez más, por lo que requieren una urgente regulación, a fin de no ampliar el ámbito de impunidad.

La experiencia, aseveró el expositor, demuestra la existencia de modalidades delictivas, hasta hace poco tiempo impensables, como por ejemplo:

1. Intervención en las líneas de comunicación de datos o teleproceso.
2. Programación de instrucciones que producen un bloqueo total al sistema.
3. Destrucción de programas por cualquier método.
4. Daño a la memoria.
5. Atentado físico contra la máquina o sus accesorios.
6. Sabotaje político o terrorismo para destruir o apoderarse de los centros computarizados.
7. Secuestro de soportes magnéticos de información valiosa con fines de chantaje (pago de rescate, etc.).
8. Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
9. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
10. Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
11. Estafas electrónicas a través de compras on line.
12. Transferencias fraudulentas de fondos.
13. Grabación de los datos de la banda magnética para su posterior utilización, a través de una nueva tarjeta o utilizando los datos en compras realizadas a través de Internet. Existen lectoras/grabadoras de bandas magnéticas.
14. Variación de los activos y pasivos en la situación contable de las empresas.
15. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
16. Lectura, sustracción o copiado de información confidencial.
17. Modificación de datos tanto en la entrada como en la salida.
18. Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
19. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
20. Uso no autorizado de programas de cómputo.
21. Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas.
22. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
23. Destrucción de datos mediante la introducción de virus, bombas lógicas, etc.
24. Uso no autorizado de información almacenada en una base de datos.
25. Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

26. Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
27. Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

CONCLUSIONES

1.- Es una conducta ilícita transnacional y sumamente lesiva, por lo que es necesario celebrar tratados de extradición o acuerdos de ayuda mutua entre los países para reducir su incidencia.

2.- La ley penal debe evitar quedar desactualizada del contexto informático en el cual se debe aplicar.

3.- Debe haber una colaboración interdisciplinaria entre el Derecho y la Ingeniería de software para diseñar mecanismos o medidas contra los delitos electrónicos, como podría ser la criptografía digital (llave: huella digital) contra el fraude en el comercio electrónico, que comprenda al correo electrónico, las actividades bancarias on line, el mercado de empresas y los servicios a los consumidores, mediante un sistema de protección de datos e identificación de socios comerciales.

****

* Doctor en Derecho, Presidente del Centro de Estudios de Criminología, Profesor de Pre y Post Grado de la Facultad de Derecho-USMP