CODIGO PENAL 130-2017. LIBRO SEGUNDO

CIBERDELITOS Y LOS DELITOS INFORMÁTICOS

Malcon Eduardo Guzmán Valladares

CIBERDELITO ≠ DELITOS INFORMATICOS

Ensayo: Cibercrimen: particularidades en su investigación y enjuiciamiento; Dra. María Concepción Rayón Ballesteros y José Antonio Gómez Hernández; Universidad Complutense de Madrid.

- **Ciberdelito o cibercrimen**: (Genero)

Cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.

Tipos de ciberdelitos: las amenazas, los delitos de exhibicionismo y provocación sexual, los delitos relativos a la prostitución y corrupción de menores, los delitos contra la intimidad, los delitos contra el honor, las estafas, los daños, los delitos relativos a la propiedad intelectual, los delitos relativos a la propiedad industrial, los delitos relativos al mercado y a los consumidores.

CIBERDELITO ≠ DELITOS INFORMATICOS

Ensayo: Cibercrimen: particularidades en su investigación y enjuiciamiento; Dra. María Concepción Rayón Ballesteros y José Antonio Gómez Hernández; Universidad Complutense de Madrid.

- **Delitos Informáticos: (Especie)**

Se producen es un ordenador o un dispositivo electrónico con conexión a Internet, bien porque el objeto sobre el que recae la conducta es el propio sistema, el programa informático o el equipo, bien porque ese sistema es utilizado como medio a través del cual se realiza la conducta delictiva o bien porque el bien jurídico protegido es la integridad de la información, la confidencialidad de la misma o los datos y los sistemas o programas informáticos.

HACKERS # CRACKERS

- **Hacking**:

Búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

A los que realizan la actividad se les conoce como hackers, los cuales pueden ser:

- Sombrero Blanco: white hat
- Sombrero Negro: black hat
- Sombrero Gris: grey hat
- Sombrero Dorado:

TIPOS DE HACKERS

- **White Hat**: Penetran la seguridad del sistema, suelen trabajar para compañías en el área de seguridad informática para proteger el sistema ante cualquier alerta.

- **Black Hat**: Conocidos como crackers muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas o creando virus, entre otras muchas cosas utilizando sus destrezas en métodos hacking.

TIPOS DE HACKERS

- **Grey Hat**: Poseen un conocimiento similar al hacker de sombrero negro y con este conocimiento penetran sistemas, cobrando luego por su servicio para reparar daños.

- **Sombrero Dorado**: Usa la tecnología para violar un sistema informático con el propósito de notificar la vulnerabilidad del sistema al administrador.

HACKERS # CRACKERS

- **Cracking**:

Conducta delictiva en la cual un individuo (denominado *Cracker*) altera, modifica, elimina o borra los datos de un programa o documento informático con la finalidad de obtener un beneficio de dicha alteración.

CLASIFICACIÓN:

- El **Password Cracking**, quebrantamiento de la seguridad de una contraseña o password;
- El **System Cracking**, quebrantamiento de la seguridad de un sistema informático; y
- El **Software Cracking**, quebrantamiento de la seguridad anticopia o antipiratería de un software.

OTRAS DENOMINACIONES DE SUJETOS ACTIVOS

- **Coders**: Se dedican hacer virus, son expertos en uno o más de un lenguaje de programación orientados a objetos.

- **Phreaking**: Persona con entendimiento de telecomunicaciones bastante amplio: clonación de teléfonos.

- **Lamer**: Considerados los más numerosos.- Personas que pretenden hacer hacking sin tener conocimientos de informática.
- Normalmente ejecutan programas hechos por los hackers.

¿NUEVOS BIENES JURÍDICOS?

Malcon Eduardo Guzmán Valladares

BIENES JURIDICOS QUE PUEDEN VERSE COMPROMETIDOS:

- Intimidad
- Propiedad
- Libertad Sexual
- La Salud
- Imagen
- Honor

- Auto Determinación Informática
- Derecho al Olvido
- Seguridad de las Redes y sistemas informáticos.

BIEN JURÍDICO: INTIMIDAD

- **Intimidad**

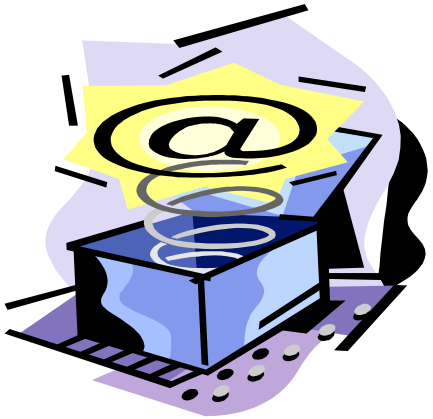
Derecho que tiene una persona natural o jurídica de que se mantenga dentro de una esfera delimitada y controlada por ésta, el conjunto de datos o informaciones que le pertenecen.

- Art. 76 Constitución de Honduras

BIEN JURÍDICO: INTIMIDAD

- ***La Criptografía***

Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados



- ***La Esteganografía***

Técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados *portadores*, de modo que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase *inadvertido* para observadores que tienen acceso a ese canal

BIEN JURÍDICO: PATRIMONIO

- Bramont-Arias y García Cantizano:

"Suma de los valores económicos a disposición de una persona, bajo la protección del ordenamiento jurídico".

- Art. 103 de la Constitución de Honduras

LA INFORMACIÓN

- El interés de la tutela de la información sería su almacenamiento, tratamiento y transmisión mediante los sistemas de procesamiento de datos por su valor económico o por describir datos personales.

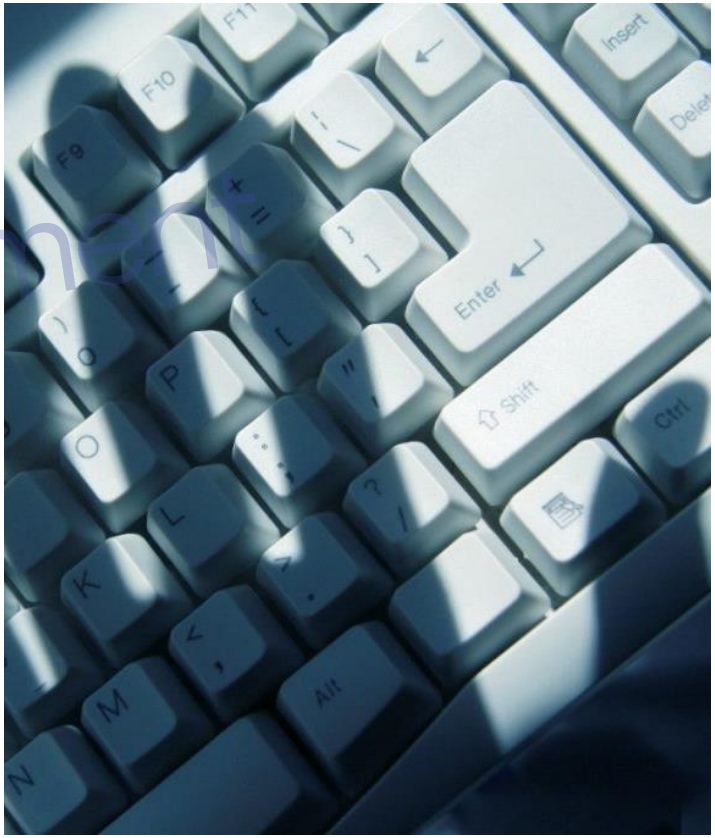
- Dr. Luis Miguel Reyna. Perú

BIEN JURÍDICO: HONOR Y DIGNIDAD

- Ana Isabel Herrán:

"Derecho que cada ser humano tiene al reconocimiento y respeto, ante él mismo y ante las demás personas, de su dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal social".

Art. 76 Constitución de Honduras



AUTODETERMINACIÓN INFORMÁTICA

- Grettel Solange:

"Derecho del individuo a controlar el uso de sus actos personales, tratados o insertos en un programa informático por el dueño de los mismos".

El término autodeterminación informática fue utilizado por primera vez el 15 de diciembre de 1983 por el Tribunal Constitucional de Karsiruhe de la República Federal de Alemania.

AUTODETERMINACIÓN INFORMÁTICA

- Habeas Data: Posibilidad jurídica de proteger el derecho de los ciudadanos a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales, con el fin de ser revisados, y si representan para la persona un perjuicio, también el ser corregidos o eliminados.

- La autodeterminación informática *"no es ningún nuevo derecho, sino que es la expresión de antiguos derechos…"* Dr. Alfredo Chirino.

SEGURIDAD DE LAS REDES Y SISTEMAS INFORMÁTICOS

BIEN JURÍDICO INTERMEDIO:

La seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos, expresada por las funciones informáticas, esto es, como ya se indicó: la integridad, confidencialidad, confiabilidad, disponibilidad, no repudio y recuperación del acceso, procesamiento, almacenamiento y la transmisión eficaz la información, los datos y los sistemas informáticos.

Se trata de un bien jurídico intermedio y autónomo, que protege de modo secundario otra clase de bienes jurídicos (personalísimos, personales y colectivos) como la intimidad personal, el patrimonio económico, la propiedad intelectual, la fe pública, etc.

SEGURIDAD DE LAS REDES Y SISTEMAS INFORMÁTICOS

COMPRENDE:

- La *confiabilidad/confidencialidad*: Derecho a que los datos o la información no sean divulgados y los sistemas espiados.

- La *integridad, exactitud y ausencia de alteraciones ilegales* de los datos: Derecho a la calidad, pureza, idoneidad y corrección de la información, de los sistemas informáticos y de los procesos de tratamiento de información.

- La *disponibilidad* de los datos e infraestructuras: Derecho que tienen los usuarios para que el uso y acceso a datos y sistemas informáticos se dé sin perturbaciones o inhibiciones violentas o abusivas por parte de terceros o incluso de injerencias por los mismos proveedores de servicios.

SEGURIDAD DE LAS REDES Y SISTEMAS INFORMÁTICOS

- Recuperación de información por parte de los usuarios en los equipos y en los distintos canales en la Web.

EL INTERNET

Malcon Eduardo Guzmán Valladares

ORIGEN: PROYECTO ARPA

- 1947.- Inicio de la Guerra Fría

- En 1957 la URSS lanzó el primer satélite: Sputnik 1.- Como respuestas los EEUU organiza la *Advanced Research Projects Agency* (Agencia de Proyectos para la Investigación Avanzada de Estados Unidos) conocida como **ARPA** y vinculada al Departamento de Defensa

- OBJETIVO: Proyecto militar para poder asegurar las comunicaciones entre diferentes puntos de Estados Unidos en caso de sufrir un ataque de gran magnitud.

ARPANET

- 1962: Paul Baran, presentó un sistema de comunicaciones que, mediante computadoras conectadas a una red descentralizada, resultaba inmune a ataques externos. En caso que uno o varios nodos resultaran destruidos, los demás se podían seguir comunicando sin problema alguno.

- 1962: Joseph Carl Robnett Licklider, del Massachusetts Institute of Technology (MIT), envió una serie de memorandos discutiendo un concepto denominado '*Galactic Network*'.

- 1965: Una Computadora TX2 de Massachusetts se conecto con una computadora Q-32 en California.

INTERNET

- 1969: Michel Elie, pionero de Internet, conecta la computadora de la UCLA con otra del SRI (Instituto de Investigación de Stanford). Poco después, cuatro universidades de EEUU estaban interconectadas. Esta red se denominó ARPANET.

- 1972: ARPANET la integran 50 universidades y centros de investigación en EEUU.

- 1973: ARPANET ya estableció conexiones con Inglaterra y Noruega.

- En 1974, la palabra 'internet' apareció por primera vez en un libro bautizado 'Internet Transmission Control Program'. Proviene del concepto 'internetworking' o 'inter-system-networking

INTERNET

- Auge de la comercialización de computadoras
- Años 80: aparecieron otras redes creando caos por la gran variedad de formatos de lenguajes informáticos.
- 1983: (Nace el Internet): Departamento de Defensa de EEUU decide usar el **protocolo TCP/IP** en su red Arpanet creando así la red Arpa Internet, lo que hoy llamamos «*Internet*»
- 2007: Lanzamiento Apple, cuyo teléfono celular permitió el acceso a internet desde un dispositivo móvil.

SERVICIOS MÁS IMPORTANTES QUE OFRECE EL INTERNET

- Correo Electrónico
- Transferencias de Archivos
- Grupos de Noticias
- Grupos de Charlas
- Acceso remoto
- Llamadas Telefónicas
- Multimedia

Informe Digital 2020, que realizan We Are Social y Hootsuite, señala que en enero de 2020 se contabilizaron 4.540 millones de internautas en el mundo, y esta cifra representa ya a más de la mitad de la población mundial (59%).

PARTES QUE INTERVIENEN EN EL FUNCIONAMIENTO DE INTERNET

Malcon Eduardo Guzmán Valladares

- Los Operadores de Telecomunicaciones
- Los proveedores de acceso a Internet
- Los proveedores de servicios de Internet
- Los suministradores de servicios en línea y suministradores de contenido
- Los usuarios

WORLD WIDE WEB

Malcon Eduardo Guzmán Valladares

INTERNET ≠ WWW

WWW: World Wide Web, es el medio global de información cuyos usuarios pueden leer y escribir a través de computadoras conectadas a Internet.

La web data de 1990 (El internet fue antes).

DIFERENCIA:

- Internet es una inmensa red de computadoras alrededor de todo el mundo conectadas entre sí;
- La web (World Wide Web) es la colección de páginas que se asienta sobre esa red de computadoras;
- Cuando se navega en el celular o en la computadora se usa el internet para acceder a la web.

WWW

METAFORICAMENTE:

- Internet: Es infraestructura: las carreteras de países de todo el mundo.

- Web: Es el contenido de las páginas web; Es lo que viaja sobre esa infraestructura: los autos, camiones, autobuses; para transportar información.

- Servidores Web: Las tiendas, las empresas, los cafés, que se asientan sobre esas vías para que los ciudadanos (los internautas) puedan entrar en las páginas web.

LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, "TIC"

Malcon Eduardo Guzmán Valladares

TIC

Las Tecnologías de la Información y la Comunicación:

Conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro.

Abarcan un abanico de soluciones muy amplio; Incluyen las

- Tecnologías para almacenar información y recuperarla después;
- Enviar y recibir información de un sitio a otro; o
- Procesar información para poder calcular resultados y elaborar informes.

TC Y TIC

Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación:

- TC: Constituidas principalmente por la radio, la televisión y la telefonía convencional
- TI: Caracterizadas por la digitalización de las tecnologías de registros de contenidos

REDES SOCIALES

Malcon Eduardo Guzmán Valladares

CRONOLOGÍA

- **Años 90**: SIXDEGREES.COM

Se basaba en la teoría de los 6 grados de separación; Permitía a sus usuarios conectarse mediante invitación con otros usuarios creando comunidad, y les permitía enviarse mensajes y ver cuando se conectaban.

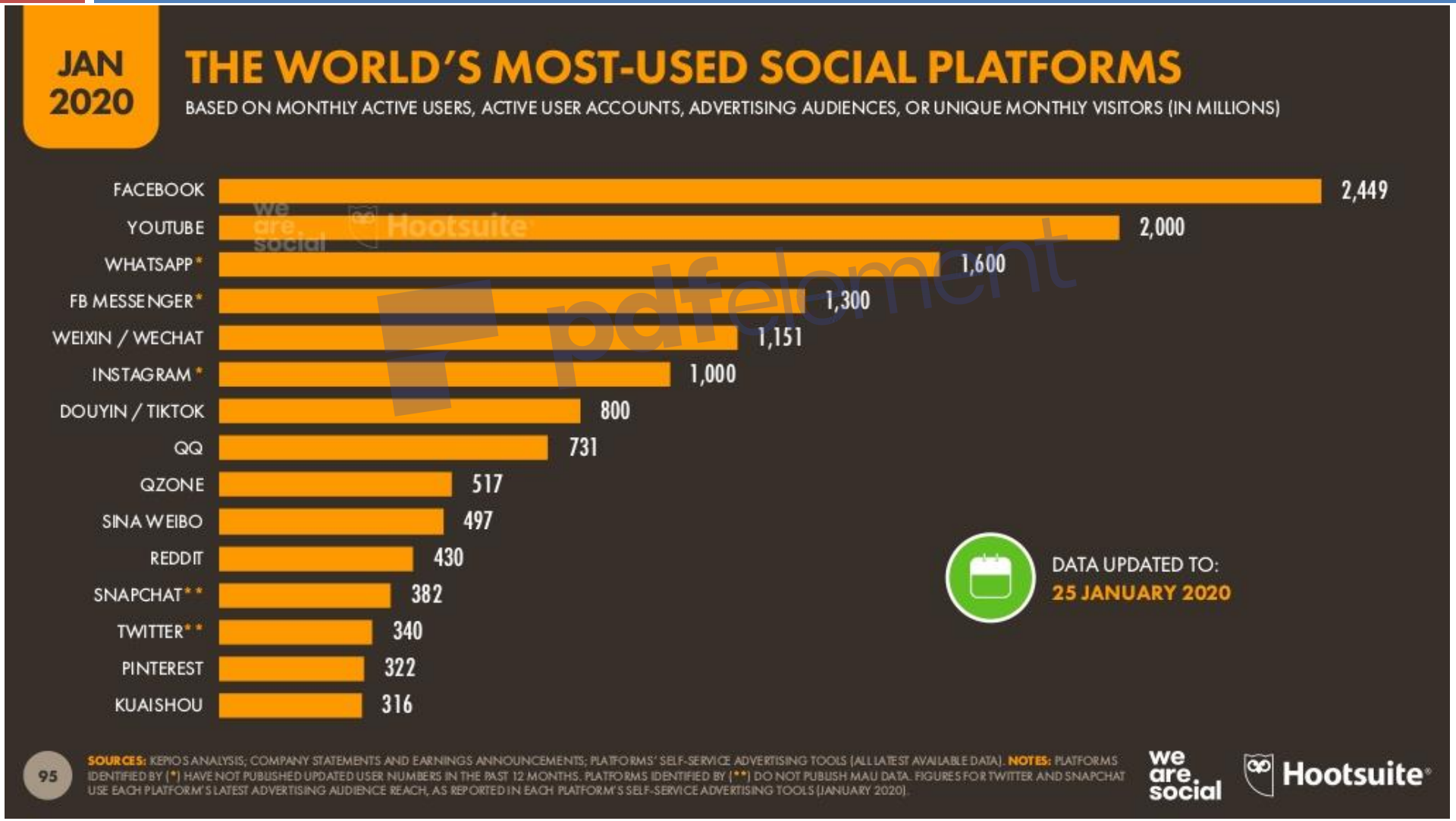
Llegó a tener más de 1 millón de usuarios, aunque desapareció en el año 2001.

- **2002**: Friendster, una red social para amantes de los videojuegos;
- **2003**: MySpace, Linkedin (red social en el ambiente del empleo);
- **2004**: Mark Zuckerberg crea Facebook
- **23/04/2005:**, se cuelga en Yotube el primer vídeo.
- **2006**: aparece la red social de microblogging Twitter

RATING DE REDES SOCIALES
Estudio Digital 2020

- **1er Lugar**: Facebook con 2.449 millones de usuarios;
- **2do Lugar**: YouTube con 2.000 millones de usuarios;
- **3er Lugar**: WhatsApp con 1,600 millones de usuarios;
- **4to Lugar**: Messenger con 1.300 millones de usuarios;
- **5to Lugar**: Instagram con 1.000 millones de usuarios;
- **8to Lugar**: TikTok con 800 millones de usuarios activos mensuales (Crecimiento del 60% en los primeros meses del 2020);
- **13vo Lugar**: Twitter con 340 millones de usuarios;

En enero de 2020, el 49% de la población mundial: 3.800 millones de personas utiliza al menos una de estas plataformas.



ATAQUES INFORMATICOS

Malcon Eduardo Guzmán Valladares

ATAQUES:

Conseguir un nivel de privilegio en el sistema que les permita realizar acciones no autorizadas

AUTORES DE LOS ATAQUES:

- Individuos con acceso autorizado al sistema.
- Individuos externos.

TIPOS DE ATAQUES:

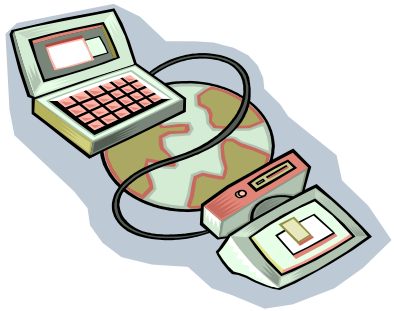
- Pasivos
- Activos

ATAQUE PASIVO

El atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Sus objetivos son la intercepción de datos y el análisis de tráfico para obtener información, como ser:

- Origen y destino de trafico;
- Hora de tráfico;
- Contenido del Tráfico;



Los ataques pasivos no provocan ninguna alteración de los datos.

ATAQUE ACTIVO

Consisten en la modificación del flujo de datos transmitido o la creación de un falso flujo de datos.- Pueden ser:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente.

- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

ATAQUE ACTIVO

- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Proceda a ingresar a X al Centro Penal" por "Proceda a liberar a X del Centro Penal".

- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo: suprimir todos los mensajes dirigidos a una determinada entidad o interrumpir el servicio de una red inundándola con mensajes espurios.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVO COMO OBJETO

- **Malware:**

Software intrusivo que afecta de manera negativa un dispositivo. Según su naturaleza puede ser utilizado para enviar spam, robar información, borrar información, acceder a cámara de manera no autorizada, destruir el dispositivo, etc.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVOS COMO OBJETIVO

- **Pheaking**:

Persona que supera la seguridad o identifica fallas en los sistemas telefónicos, que le permite obtener privilegios no accesibles de forma legal.

- **Ransomware**

Este tipo que consiste en que toda la información una computadora o dispositivo queda *'atrapada'* o cifrada, y la víctima tiene que pagar una suma de dinero al hacker para recuperarla. (Ciberextorsión).

- **Ataque DDoS (Distributed Denial of Service)**

Consiste en sabotear un sitio Web mediante la saturación de paquetes de información al grado de colapsar los servidores para dejarlo fuera de línea.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVOS COMO OBJETIVO

- ***Carding***: Sustracción de datos relacionadas con tarjeta de crédito, para poder acceder al dinero de las personas.- Es el uso no autorizado de tarjetas de crédito.

El *Carding*, puede ser realizado mediante:

- ***Pharming*:** Utiliza malware para redirigir a los usuarios desprevenidos hacia versiones falsificadas de sitios web, con el fin de que introduzcan sus datos personales.

- ***Keylogging*:** Este tipo de malware (o, para ser más específicos, de spyware) registra en secreto todo lo que escribe para obtener información de sus cuentas y otros datos personales.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVOS COMO OBJETIVO

- ***Phising***: que son correos electrónicos o páginas web con links que tienen una apariencia de pertenecer a una institución legítima, como bancos, universidades, hoteles o tiendas online, para que la persona ingrese datos;

- ***Smishing***: Variante del *phishing* que consiste en que por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número o que se entre a un sitio web.
- Se intenta suplantar la identidad de alguna persona conocida de los contactos o de una empresa de confianza.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVOS COMO OBJETIVO

Smishing: Ejemplos:

- *"Ha sido ud inscrito en nuestro servicio Prime Video por cable a un costo de $10.00 mensuales; Para cancelar el servicio visite nuestra página web: www.?????.com."*

- *"Banco XXX le informa que su refinanciamiento por L. 50,000.00 ha sido aprobado. Solicite mayor información por mensaje de texto (SMS) al teléfono XXXXXX"*

- *"María: Anoche realmente me sentí ofendida; deseo que aclaremos las cosas; Llámame al teléfono XXXXX"*

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVO COMO INSTRUMENTO

- **Cyberbulling**

Acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

(Las Tecnologías de la Información y la Comunicación: TIC)

- **Grooming**

Serie de conductas y acciones emprendidas por un adulto con el objetivo de ganarse la confianza de un menor de edad, creando una conexión emocional con el fin de disminuir las inhibiciones del menor y poder abusar sexualmente de él.

ALGUNOS TIPOS DE ATAQUES
DISPOSITIVO COMO INSTRUMENTO

- **Sexting**

Envío de contenido multimedia con imágenes personas de desnudez, eróticas o sexuales.

- **Revenge Porn (Porno Vengativo)**

Conducta estrechamente ligada al sexting.

El Revenge Porn es el contenido sexual explícito que se publica en internet sin el consentimiento de la persona que aparece representada.

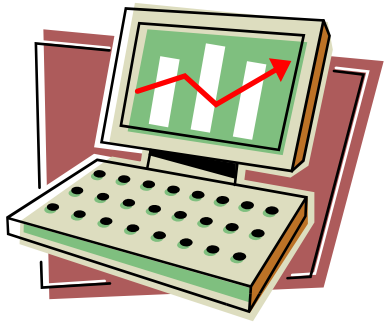
La víctima se ve sometida a una situación de exposición no consentida de su sexualidad, lo que constituye violencia sexual psicológica.

CIBERDELITOS Y DELITOS INFORMÁTICOS

Malcon Eduardo Guzmán Valladares

CARACTERÍSTICAS GENERALES

NATURALEZA



- ¿Delitos de Cuello Blanco?
- ¿Son de carácter doloso o Imprudentes?

CARACTERISTICAS

- Sujetos Activos con conocimientos informáticos
- Maximación de los Daños Económicos
- Facilidad de tiempo, espacio y muchas veces dinero.
- Facilidad de distancia y anonimato;
- Alta cifra negra
- Requiere especialistas para su investigación y para la recolección de la prueba.

ASPECTOS QUE INFLUYEN EN SU DESARROLLO

- El Desarrollo Tecnológico
- Globalización de Mercados y Economía
- Masificación de la Información
- La transnacionalización de los delitos

POLÍTICA CRIMINAL Y LABOR LEGISLATIVA

- Justificación de su inclusión en el Código Penal:
  - La computadora y los celulares pueden ser instrumento u objeto material del delito;
  - Impunidad por atipicidad de los ámbitos situacional de las figuras incriminatorias tradicionales;
  - Impunidad ante la prohibición de aplicación por *analogía in mala partem* de las figuras tradicionales;
  - Graves daños a los bienes jurídicos;

CIBERDELITO

- **Organización de Cooperación y Desarrollo Económico:**

"Cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos o la transmisión de datos".

- **Klaus Tiedeman (Alemania):**

"Todos los actos antijurídicos según la ley penal vigente (o socialmente dañosos y por eso penalizables en el futuro) realizado con el empleo de un equipo de procesamientos de datos".

- **ARTEAGA:**

"Toda acción u omisión dolosa o imprudente, típica, antijurídica y culpable, realizada por una persona, que cause un perjuicio a personas naturales o jurídicas, con animo de lucro o sin él, o que se agencie un beneficio en forma ilícita, en el que se cuenta con una computadora como medio o fin indispensable del mismo" .

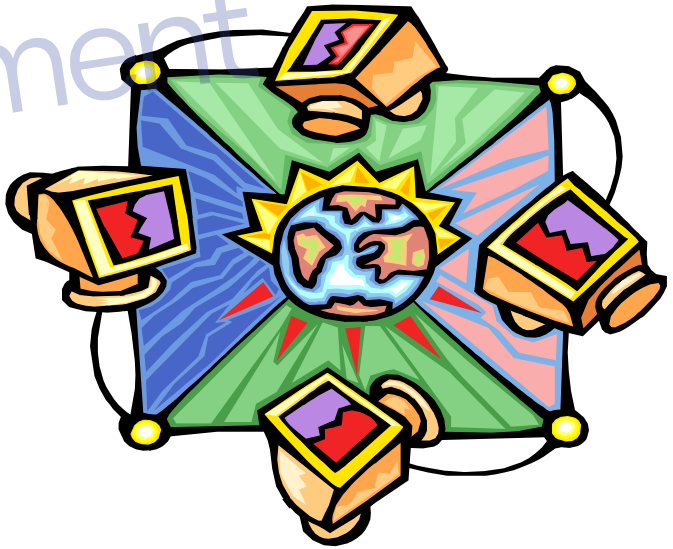
CIBERDELITOS MÁS COMUNES

- **FRAUDE INFORMATICO**: Es el conjunto de conductas maliciosas, que valiéndose de cualquier manipulación fraudulenta, modifiquen o interfieran en el funcionamiento de un programa informático, telemático o alguna de sus partes componentes, para producir un perjuicio económico de cualquier índole.

- **PIRATERÍA INFORMATICA**: Reproducción plagio, distribución, comunicación, transformación, exportación o importación de software, sin autorización con o sin animo de lucro.

DELITOS INFORMATICOS MÁS COMUNES

- **ESPIONAJE INFORMÁTICO**: Consiste en obtener sin autorización datos almacenados, en un fichero automatizado, en virtud de lo cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento automatizado de la misma.



DELITO INFORMÁTICO

- **Nuria Matellanes (España):**

"Conductas que constituyen agresiones a las funciones de procesamiento, transmisión y ejecución de programas propios de sistemas informáticos.".

DELITOS INFORMÁTICOS QUE DEBEN DE SER PENALIZADOS

- Conductas que afecte un dispositivo en su materialidad o funcionalidad;
- Conductas que afecten la integridad y/o autenticidad de los documentos informáticos;.
- Conductas consistentes en el acceso y/o utilización abusiva de dispositivos;
- Conductas que afecten el normal funcionamiento normal de un sistema electrónico;
- Conductas que violenten la intimidad de las personas y la reserva de la información;

- Como Agravante: conductas que impliquen la ejecución de delitos tradicionales utilizando como instrumento dispositivos informáticos.

CARACTERÍSTICAS GENERALES

La fenomenología delictiva vinculada a las nuevas tecnologías de la información y las comunicaciones es cada vez más variada y abundante y que cualquier regulación queda pronto anticuada.

La técnica legislativa penal debe de hacer uso a tipos penales abiertos y tipos penales en blanco.

CLASIFICACIÓN

- **SEGÚN EL FIN**
- El dispositivo como Instrumento o medio.
- El dispositivo como fin u objeto.

- **SEGÚN EL METODO:**
- Conductas vinculadas a la fase de acceso de las redes o sistemas informáticos
- Conductas vinculadas al tránsito de la información a través de las redes o sistemas informáticos

DATOS BASICOS EN LA INVESTIGACIÓN DE CIBERDELITOS

- La dirección IP asignada al sospechoso por el proveedor y los datos contractuales (nombre y dirección) junto con la hora, fecha y duración de la comunicación, la concreta transacción o intercambio realizado.

- La localización geográfica desde la que se conecta el sospechoso con el proveedor.

- Las cuentas corrientes asociadas al pago de los servicios.

- El número de teléfono de origen y destino de las comunicaciones realizadas por el sospechoso.

DATOS BASICOS EN LA INVESTIGACIÓN DE CIBERDELITOS

- La copia de los ficheros de que disponga el sospechoso en su espacio web.
- Las llamadas perdidas con determinación de su hora, duración y frecuencia.
- El tipo de servicio telefónico empleado por el sospechoso.
- El identificador del equipo en los teléfonos móviles.
- Los datos de fecha y momento de activación de la tarjeta prepago de móviles, etc.

CONVENIO SOBRE LA CIBERDELINCUENCIA DEL 23 DE NOVIEMBRE DE 2001 Y SU PROTOCOLO ADICIONAL DE 2003

CONVENIO DE BUDAPEST

Malcon Eduardo Guzmán Valladares

CONVENIO DE BUDAPEST

- La Convención tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de estos delitos y establecer un régimen efectivo de cooperación y asistencia internacional.

- A la fecha ha sido ratificado por 60 Estados, entre ellos los latinoamericanos: República Dominicana, Chile, Argentina, Colombia.

- Honduras no lo ha ratificado.

NOS SIRVE DE GUÍA CONCEPTUAL

DISPOSICIONES PROCESALES

- Conservación rápida de datos informáticos almacenados, incluido el tráfico de datos (Artículo 16°);
- Conservación y revelación parcial rápidas de los datos sobre tráfico (Artículo 17°);
- Obligatoriedad de personas y proveedores de servicios de presentar la información requerida (Artículo 18°); ·
- Registro de todo tipo de dispositivo o sistema de almacenamiento informático y la confiscación de los datos informáticos almacenados en ellos (Artículo 19°);
- Obtención en tiempo real de datos relativos al tráfico (Artículo 20°); y
- Interceptación de datos relativos al contenido de las comunicaciones (Artículo 21°).

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Acceso ilíc**ito (Art. 2): Tipificación del acceso deliberado e ilegítimo a todo o parte de un sistema informático.

- **Interceptación ilícita** (Art. 3): Tipificación de la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo;

- **Ataques a la integridad de los datos (Art. 4):** Tipificación de todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos;

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Ataques a la integridad del sistema (Art. 5):** Tipificación de la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.;

- **Abuso de los dispositivos (Art. 6):** Producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos informáticos.

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Abuso de los dispositivos (Art. 6):** Producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer delitos informáticos.

- **Abuso de los dispositivos (Art. 6):** Posesión de cualquier dispositivo, incluido un programa informático, contraseña, código de acceso o datos informáticos similares con intención de que sean utilizados para cometer delitos informáticos.

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Falsificación informática (Art. 7):** Tipificación de la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

- **Fraude informático (Art. 8):** Tipificación de los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:
  - a) la introducción, alteración, borrado o supresión de datos informáticos;
  - b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Delitos relacionados con la pornografía infantil (Art. 9):** Tipificación de la comisión deliberada e ilegítima de los siguientes actos:
  - a) producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
  - b) oferta o puesta a disposición de pornografía infantil a través de un sistema informático;
  - c) difusión o transmisión de pornografía infantil a través de un sistema informático;
  - d) adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
  - e) posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

DISPOSICIONES PENALES.- TIPIFICACIÓN

- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (Art. 10).** Tipificación de las infracciones de la propiedad intelectual que defina su legislación.

- **PROTOCOLO ADICIONAL**: Tiene por objeto armonizar la legislación penal sustantiva en relación a la lucha contra el racismo y la xenofobia en Internet

CÓDIGO PENAL 144-1983
CIBERDELITOS Y DELITOS INFORMÁTICOS

Malcon Eduardo Guzmán Valladares

CÓDIGO PENAL 144-1983

- **Art. 147-C**.- Hostigamiento Sexual
- **Art. 149-D**.- Pornografía Infantil
- **Art. 214**.-Intercepción de correspondencia
- **Art. 223 último párrafo**.- Hurto de señales;
- **Art. 242.14**.- Fraude de Telecomunicaciones;
- **Art. 254 segundo párrafo**.- Daño Informático;

CÓDIGO PENAL 144-1983

- **Artículo 394-E**.- Destrucción, ocultamiento, falsificación de información financiera para obtener un crédito;

- **Artículo 394-F**.- Ocultamiento de irregularidades en la actividad financiera;

- **Artículo 394-I**.- Utilización indebida de sistemas de procesamiento de datos

CONCEPTOS
CÓDIGO PENAL 130-2017

Malcon Eduardo Guzmán Valladares

ARTÍCULO 405

- **Datos Informáticos**: las unidades básicas de información, cualquiera que sea su contenido, expresados en una forma que permita su tratamiento por un sistema de información, incluyendo los programas que hacen posible que esta función se lleve a cabo;

- **Sistema Informático**: un dispositivo o conjunto de dispositivos interconectados o relacionados entre sí, que permiten, gracias a un programa, el tratamiento automatizado de datos informáticos, de manera que abarca tanto el hardware como el software necesario para su funcionamiento;

ARTÍCULO 405

- **Programa Informático**:

La secuencia de instrucciones o indicaciones necesarias para que el sistema informático pueda realizar una función o una tarea u obtener un determinado resultado.

CIBERDELITOS

DELITOS EJECUTADOS MEDIANTE TECNOLOGÍA DE LA INFORMACIÓN

Malcon Eduardo Guzmán Valladares

CONSIDERANDO 1

- *Que en los últimos treinta (30) años hemos experimentado alteraciones en la conducta social, específicamente en la conducta delictiva que son atribuibles, entre otros factores,* [por] *el dominio de tecnologías avanzadas particularmente las relativas a la informática y las telecomunicaciones, […] que generan resultados y hábitos positivos e igualmente resultados y hábitos negativos, muchos de estos últimos manifestados en el aparecimiento de nuevas figuras delictivas.*

LIBRO I.- REGULACIONES GENERALES

Art.- 51.- Pena de Prohibición de Comunicación con la víctima.

La prohibición de comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Órgano Jurisdiccional competente, impide al condenado establecer con ellas, por cualquier medio de comunicación, informático o telemático, contacto verbal, escrito o visual.

LIBRO II.- TIPIFICACIONES

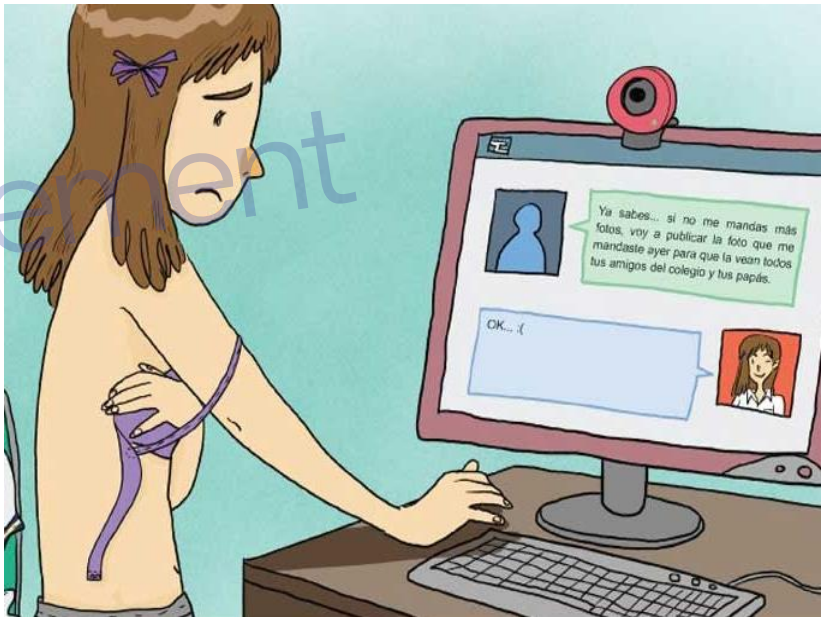
ARTÍCULO 232.- CONCEPTO DE PUBLICIDAD. Las injurias y calumnias se entienden hechas con publicidad cuando se efectúan a través de impresos, televisión, radio, Internet, redes de información, ante una multitud de personas o a través de otros medios de eficacia semejante.

ARTÍCULO 246.- AMENAZAS. Si la amenaza se realiza […] a través de medios informáticos, audiovisuales o telemáticos, las penas previstas se deben aumentar en un tercio (1/3).

LIBRO II.- TIPIFICACIONES

ARTÍCULO 253.- Contacto con finalidad sexual con menores por medios electrónicos.

Quien, a través de las tecnologías de la comunicación e información, propone a un menor de catorce (14) años concertar un encuentro físico para realizar actividades sexuales, siempre y cuando tal propuesta se acompañe de actos materiales encaminados a dicho encuentro, debe ser castigado con la pena de arresto domiciliario de uno (1) a tres (3) años.



LIBRO II.- TIPIFICACIONES

ARTÍCULO 262.- Concepto de Pornografía Infantil.

A los efectos de lo dispuesto en este capítulo, se entiende por pornografía infantil cualquier material donde se utilice la persona o la imagen de persona, por medio directo, mecánico o con soporte informático, eléctrico, audiovisuales o de otro tipo, que con finalidad de excitación sexual, recoge cualquier clase de actos sexuales o conductas sexualmente explícitas, realizados por menores de dieciocho (18) años con otras personas, mayores o menores de edad, o con ellos mismos, así como la reproducción de sus órganos sexuales o, eventualmente, de otras partes del cuerpo en un contexto sexual.

LIBRO II.- TIPIFICACIONES

ARTÍCULO 272.- Descubrimiento y revelación de secretos.

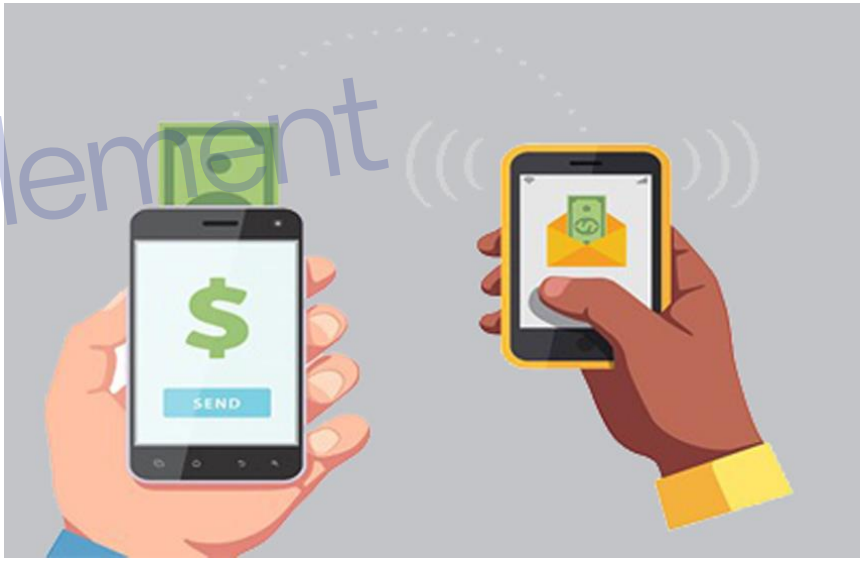
Debe ser castigado con las penas de dos (2) a tres (3) años de prisión y multa de trescientos sesenta (360) a setecientos veinte (720) días quien, en perjuicio de terceros y sin estar autorizado, accede, se apodera, altera o utiliza datos personales incorporados a ficheros, soportes, registros informáticos, electrónicos, telemáticos o a cualquier otro tipo de archivo o registro público o privado.

Artículo 276.- Agravantes Específicas.

LIBRO II.- TIPIFICACIONES

ARTÍCULO 365.- ESTAFA. También se comete el delito de estafa en los casos siguientes:

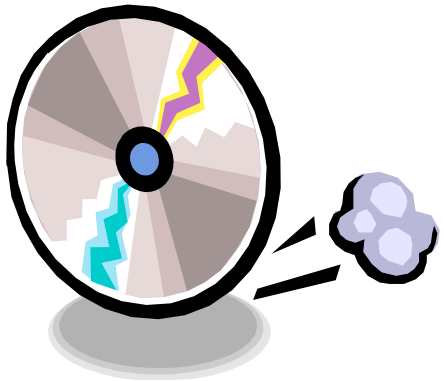
Quien con el propósito de obtener un provecho ilícito consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante una manipulación informática o el uso de otro artificio semejante; y,



ARTÍCULO 392.- ELUSIÓN DE MEDIDAS TECNOLÓGICAS

Software Cracking

Quien, sin autorización de los respectivos titulares, con ánimo de lucro y en perjuicio de tercero elude o evade cualquier medida tecnológica eficaz que esté dirigida a impedir la vulneración de los derechos de autor y derechos conexos, debe ser castigado con las penas de prisión de uno (1) a tres (3) años y multa por una cantidad igual o hasta el triple del beneficio obtenido.



ARTÍCULO 392.- ELUSIÓN DE MEDIDAS TECNOLÓGICAS

Facilitación de Software Cracking

Con las penas de prisión de uno (1) a dos (2) años y multa por una cantidad igual o hasta el triple del beneficio obtenido se debe castigar a quien elabora, fabrica, reproduce, distribuye, importa o exporta, o pone a disposición del público con una finalidad comercial, con ánimo de lucro y en perjuicio de tercero, cualquier programa, herramienta, medio o procedimiento, dirigido a facilitar de forma ilegítima la supresión o neutralización de cualquier medida tecnológica específicamente destinada a impedir la vulneración del derecho de autor y derechos conexos.

LIBRO II.- TIPIFICACIONES

ARTÍCULO 395.- Descubrimiento y revelación de secreto industrial o comercial.

Quien para obtener ilegítimamente un secreto de empresa se apodera por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, intercepta las comunicaciones o de cualquier otro modo ilegítimo se procura dicha información reservada, debe ser castigado con las penas de prisión de dos (2) a cuatro (4) años y multa por una cantidad igual o hasta el triple del beneficio obtenido.

LIBRO II.- TIPIFICACIONES

ARTÍCULO 450.- Fabricación o tenencia de instrumentos para la falsificación de moneda.

La elaboración o tenencia de útiles, materiales, instrumentos, aparatos, sustancias, datos, programas informáticos u otros medios específicamente dedicados por naturaleza o destino a la falsificación de moneda, se debe castigar con la pena de prisión de cuatro (4) a seis (6) años.

LIBRO II.- TIPIFICACIONES

ARTÍCULO 466.-

Fabricación o tenencia de instrumentos para la falsificación de tarjetas bancarias y cheques de viaje.

La elaboración o tenencia de útiles, materiales, instrumentos, aparatos, sustancias, datos, programas informáticos u otros medios específicamente dedicados por naturaleza o destino a la falsificación, se deben castigar con la pena de prisión de cuatro (4) a seis (6) años.

LIBRO II.- TIPIFICACIONES

Artículo 579.- Introducción de objetos prohibidos.

El que ilícitamente introduzca, trate de introducir o permita que otro introduzca en centros penitenciarios, granjas penales, centros preventivos o en los centros de internamiento de niños, objetos prohibidos en materia de informática y telecomunicaciones que permitan la emisión y recepción de datos por medio de voz, datos o imágenes, debe ser castigado con la pena de tres (3) a cinco (5) años de prisión y multa de quinientos (500) a mil (1000) días.

.

LIBRO II.- TIPIFICACIONES

Artículo 579.- Introducción de objetos prohibidos.

El que ilícitamente introduzca, trate de introducir o permita que otro introduzca en centros penitenciarios, granjas penales, centros preventivos o en los centros de internamiento de niños, objetos prohibidos en materia de informática y telecomunicaciones que permitan la emisión y recepción de datos por medio de voz, datos o imágenes, debe ser castigado con la pena de tres (3) a cinco (5) años de prisión y multa de quinientos (500) a mil (1000) días.

.

DELITOS INFORMÁTICOS

CÓDIGO PENAL 130-2017
TÍTULO XXII.- SEGURIDAD DE LAS REDES Y DE LOS SISTEMAS INFORMÁTICOS

Malcon Eduardo Guzmán Valladares

TIPOLOGIAS

- Acceso no autorizado a sistemas informáticos (Art. 398)
- Daños a datos y sistemas informáticos (Art. 399)
- Abuso de dispositivos (Art. 400)
- Suplantación de Identidad (Art. 401)
- Ciberterrorismo o terrorismo electrónico (Art. 592)

ARTÍCULO 398.- ACCESO NO AUTORIZADO A SISTEMAS INFORMÁTICOS

System Cracking: Debe ser castigado con pena de prisión de seis (6) a dieciocho (18) meses o multa de cien (100) a doscientos (200) días quien, vulnerando las medidas de seguridad establecidas para impedirlo, accede sin autorización a todo o en parte de un sistema informático.

La pena del párrafo anterior se debe aumentar en un tercio (1/3) si el sistema al que se accede se refiere a estructuras o servicios esenciales para la comunidad.

- **Sujeto Activo**: Persona distinta a la que tenga acceso vigente;
- **Conducta Criminosa**: Vulnerar las medidas de seguridad del sistema
- **Delito de Resultado**; Admite Tentativa;
- **Delito de Peligro**;

ARTÍCULO 399.- DAÑOS A DATOS Y SISTEMAS INFORMÁTICOS

- **Daños**: Quien por cualquier medio y sin autorización introduce, borra, deteriora, altera, suprime o hace inaccesible de forma grave datos informáticos, debe ser castigado con la pena de prisión de uno (1) a dos (2) años o multa de cien (100) a trescientos (300) días.

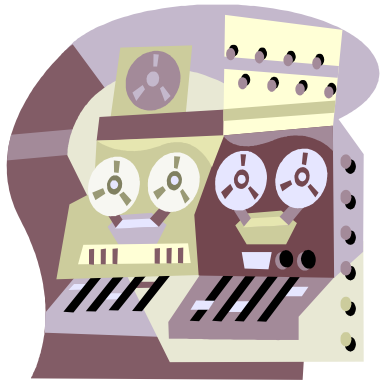
- **Ransomware:** Quien sin estar autorizado inutiliza, total o parcialmente, el funcionamiento de un sistema informático, impidiendo el acceso al mismo o imposibilitando el desarrollo de alguno de sus servicios, debe ser castigado con la pena de prisión de uno (1) a tres (3) años o multa de cien (100) a cuatrocientos (400) días.

ARTÍCULO 400
ABUSO DE DISPOSITIVOS

Malcon Eduardo Guzmán Valladares

La fabricación, importación, venta, facilitación o la obtención para su utilización de dispositivos, programas informáticos, contraseñas o códigos de acceso, destinados o adaptados para la comisión de los delitos de daños informáticos o de acceso ilícito a sistemas informáticos, debe ser castigada con la pena de prisión de seis (6) meses a un (1) año o multa de cien (100) a doscientos (200) días.

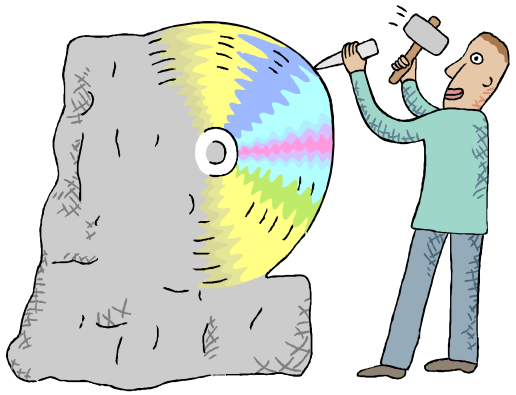
- Delito de Peligro
- Delito de Mera Actividad
- Delito con Dolo Reforzado



ARTÍCULO 401
SUPLANTACIÓN DE IDENTIDAD

Debe ser castigado con la pena de prisión de seis (6) meses a un (1) año o multa de cien (100) a trescientos (300) días, quien con ánimo defraudatorio y a través de las tecnologías de la información y la comunicación, suplanta la identidad de una persona natural o jurídica.

- Delito de Mera Actividad
- Delito de Peligro



ARTÍCULO 592.- CIBERTERRORISMO O TERRORISMO ELECTRÓNICO

Quien por cualquier medio o procedimiento y sin autorización, accede a un sistema informático de la Administración Pública del Estado o que preste servicios de carácter estatal, impide el acceso al mismo o altera o daña datos en él contenido concurriendo algunas de las finalidades del terrorismo, debe ser castigado con las penas de prisión de cuatro (4) a seis (6) años y multa de trescientos (300) a mil (1000) días.

ARTÍCULO 404
JURISDICCIÓN

Los Órganos Jurisdiccionales nacionales deben conocer de los delitos informáticos, cuando se ejecuten en los casos siguientes:

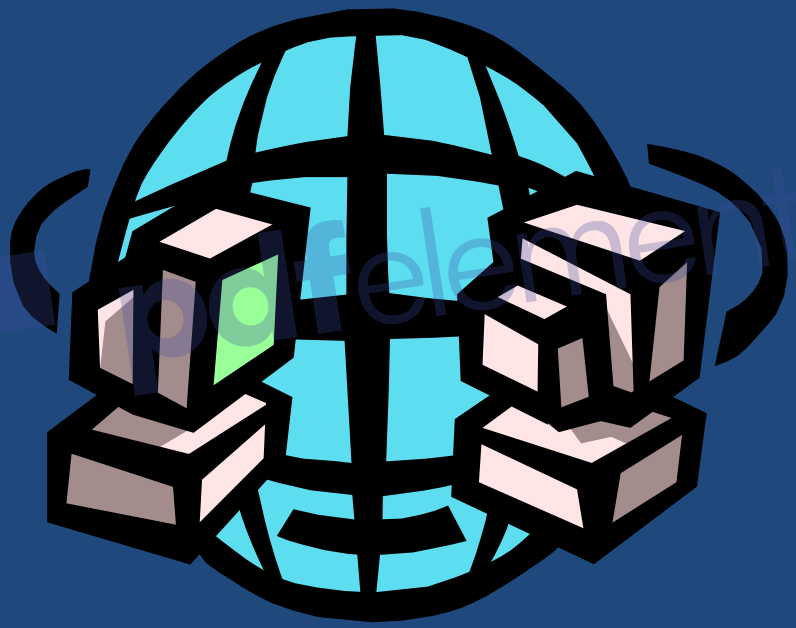
- **Por el Lugar donde se Desarrollo la conducta**: En Honduras, aunque se dirijan contra datos o sistemas informáticos situados fuera de éste; o,

- **Por el Lugar del resultado o donde se esperaba el resultado:** Contra datos o sistemas informáticos situados en Honduras, aunque el culpable hubiese actuado desde fuera del territorio nacional.

COMPARATIVO DE TIPIFICACIONES

CONDUCTA 101	CONVENIO DE BUDAPEST	CÓDIGO PENAL 130-2017	ALCANCE DE LA NORMA
Acceso Ilícito	Art. 2	Art. 398	Igual
Intercepción Ilícita	Art. 3	Art. 272 y 395	Limitado
Ataque a la Integridad de los Datos	Art. 4	Art. 399 primer párrafo	Igual
Ataque a la Integridad del Sistema	Art. 5	Art. 399 segundo párrafo	Igual
Abuso de Dispositivos	Art. 6.a	Art. 400	Igual
Abuso de Dispositivos	Art. 6.b	Art. 450 y 466	Limitado
Falsificación Informática	Art. 7	Art. 399	Muy Limitado
Fraude Informático	Art. 8	Art. 365, 399, 401	Muy Limitado
Pornografía Infantil	Art. 9	Art. 261 y 262	Igual
Delitos contra la Propiedad Intelectual	Art. 10	Art. 392	Limitado

CONCLUSIONES



Malcon Eduardo Guzmán Valladares

CONCLUSIONES

- Los ciberdelitos lesionan o ponen en peligro bienes ya reconocidos por la legislación actual. Se requiere la redefinición de los alcances de aquellos bienes jurídicos ya identificados.

- Se debe de entender que los delitos informativos protegen la seguridad de las redes y sistemas informáticos como bien jurídico intermedio.

- El ciberdelito no debe comprenderse como toda conducta ilícita que involucre el uso de un dispositivo (lo que antes se conocía como delitos computacionales), sino sólo aquellas en donde el medio informático permita su comisión y que éste sea necesario también para su investigación.

CONCLUSIONES

- Al crearse internet se facilita que los datos personales sean obtenidos indebidamente y utilizados para fines diferentes de los cuales fueron creados, lesionándose con ello, uno de los bienes más preciados como es el derecho a la intimidad y con ello limitando al individuo dueño de sus datos personales, su derecho a la autodeterminación informática.

- Los ciberdelitos son actualmente cometidos por personas con conocimientos medios o altos sobre datos y sistemas informáticos, pero en la medida de que el conocimiento de la informática se difunda, se volverán más comunes.

CONCLUSIONES

- El internet debe de ser regulado, como de igual forma es regulada la conducta que en el mundo material pueda constituir delito. Todo aquello que rija en el mundo real, debe igualmente regir el internet y la web. Por tanto, la protección de los derechos fundamentales de los ciudadanos ha de extenderse a este nuevo medio.

- Ante la transnacionalización de las criminalidad informática, los Estados, sin perder su soberanía, deberán unificar sus regulaciones internas y a nivel externo establecer Tratados Internacionales y/o Convenios de Extradición, que faciliten la persecución de los responsables y la prevención de los mismos.

CONCLUSIONES

- El Código Penal 130-2017 crea figuras delictivas en donde las tecnologías de la información son tanto instrumentos como fin de la conducta delictiva; Empero es aconsejable mejorar las mismas adaptándolas a las figuras definidas en el Convenio de Budapest.

- Dadas las características de esta problemática sólo a través de una política criminal integral, que abarque los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos y no encomendarle ésta tarea al derecho penal exclusivamente

TEMAS DE LA PROXIMA CHARLA

- Código Penal Parte Especial
  - Delitos en contra el Orden Socio Económico: El Lavado de Activos

CONTACTO

Malcon Eduardo Guzmán Valladares

eduardoguzman819@Gmail.com