El Mundo Digital y la Guardia Civil

JOSE GIMÉNEZ REYNA RODRÍGUEZ

Teniente Coronel de la Guardia Civil

1.- CONSIDERACIONES SOBRE EL CONCEPTO DE DELITO INFORMÁTICO.

Diariamente, en el mundo actual grandes cantidades de asientos financieros son almacenados, manipulados y transmitidos por medio de ordenadores y redes telemáticas asociadas. Las entidades financieras a nivel mundial transmiten diariamente trillones de transacciones financieras a través de las redes informáticas.

La información relacionada con el diseño de nuevos productos en la industria, medicina, seguros, investigación científica, política social, política de Justicia o la Defensa nacional por poner algunos ejemplos, va dejando paulatinamente de transmitirse a través de documentos entre despachos o gabinetes para pasar a almacenarse y circular a través de redes informáticas.

Las denominadas redes informáticas han evolucionado prodigiosamente. Podríamos decir que la informática es una ciencia moderna y que su implantación en España es realmente muy actual destacando varias etapas cuyos límites son muy difusos:

1.960-1.970 : Existencia de grandes ordenadores (Mainframe) adquiridos en EEUU con relativo "poder de cálculo" asociados a Empresas Instituciones y Centros Neurálgicos de la Defensa. (Universidades, Bancos, etc.).

1.970-1.980 : Mejora de los grandes ordenadores y diferenciación entre:

-Grandes ordenadores (Mainframe). Ligados a Instituciones y grandes empresas.

- Miniordenadores. Ordenadores de tipo medio, base y soporte de las primeras redes informáticas en el ámbito nacional en empresas e instituciones.

- Microordenadores (Personal Computer). Ordenadores personales a nivel usuario que permiten llevar la informática básica a los hogares.

1.980- 1.990: Gran auge de la informática a nivel usuario con la implantación del P.C. a nivel nacional y la aparición de software más adaptado al consumidor (Windows, Mac, etc.).

La primera implantación en España de INTERNET fue a finales de los ochenta.

Internet es una red informática mundial cuyos orígenes hay que buscarlos en una red informática establecida entre Universidades e Instituciones de EEUU denominada ARPANET (1.969). Posteriormente se adopta en esta red la utilización del protocolo de comunicaciones TCP/IP que le permite ganar potencia y globalidad en las comunicaciones entre ordenadores produciéndose la exportación de esta Tecnología al resto del mundo.

1.990 - 2.000: Explosión en el uso de Internet al definirse la filosofía proveedor (empresa de servicios de Internet que cuanta con Miniordenadores que se conectan a otros proveedores formando una malla mundial) y usuarios (Persona física o JURIDICA que contrata los servicios de Internet con un proveedor para lo cual solo necesita un microordenador o P.C adecuado, un software o programas proporcionados por el proveedor y un módem para conectarse al proveedor a través de la red telefónica básica (RTB) o una tarjeta RDSI si se desea conectar a través de una línea dedicada digital ganando en velocidad de comunicación.

Los servicios proporcionados por los proveedores de Internet son muy variados y evolucionan prácticamente día a día pero los más comunes son los siguientes:

Páginas WEB: Cada Usuario cuenta con un espacio cedido en el, ordenador del proveedor para "colocar" y poner a disposición del resto de los usuarios de la red a nivel mundial una o varias páginas electrónicas denominadas WEB que permiten difundir información (texto, fotografías, sonido, vídeo, etc.) o acceder a servicios (mediante la introducción de los datos de un medio de pago se consigue un servicio tal como una entrada a un concierto, la compra de un libro, de un coche, jugar a la lotería, realizar una transferencia bancaria, etc.).

- Correo electrónico E-MAIL: Cada usuario cuenta con al menos una "cuenta" de correo electrónico en el ordenador-servidor del proveedor que corresponde a una dirección.

Por ejemplo:

manuel.plaza@arrakis.es (cuenta de correo del usuario "Manuel Plaza" en el ordenador del proveedor "arrakis" en "es" España).

sculptures@sothebys.uk (cuenta de correo del usuario "sculptures"- Departamento de Esculturas" del ordenador del proveedor "Sothebys" - Galería de Obras de Arte - en "uk" Reino Unido).

Los mensajes de correo electrónico son confeccionados por los usuarios origen que los transmiten siempre hasta su proveedor (en servicio durante 24 horas) y posteriormente es éste quien los transmite hasta el proveedor destino (en servicio durante 24 horas) de tal forma que el usuario destinatario, pese a que tenga su ordenador personal apagado recibe correo electrónico en su cuenta del proveedor y puede "bajarlo" a su ordenador cuando desee.

A través de correo electrónico pueden enviarse documentos, libros, fotografías, videos, sonidos, etc.

- FTP: (File Transfering Program)

Es una utilidad asequible en INTERNET a través de la cual se pueden transferir bloques de información entre proveedores y usuarios en pocos segundos entre cualquier parte del mundo

- IRC (Chat).

Utilidad de INTERNET que permite a dos o más usuarios establecer una comunicación en directo entre puntos existentes en cualquier punto del globo. Los contactos se producen a través de canales específicos y los usuarios normalmente utilizan sobrenombres o "nicknames".

A su vez al mismo tiempo que se producen charlas o "chats" entre dos o más interlocutores pueden enviarse fotografías, videos sonidos, textos etc.

- NEWS

Las denominadas "news" son consideradas foros de debate sobre los temas más diversos donde los usuarios de la red pueden acceder para conocer las últimas novedades sobre un tema e incluso añadir artículos o comentarios al mismo.

Existen multitud de foros de debate (más de 30.000 a nivel mundial) y algunos tan particulares como aquellos donde se vierte todo tipo de información sobre "pedofilia" "sexo con niños" "química de drogas" etc.

- TELNET.

Todos los usuarios de INTERNET son identificados por un número correspondiente a su ordenador denominado IP que puede ser fijo o variable. Este número es asignado por el proveedor a cada usuario y a su vez cada proveedor tiene asignado a nivel internacional un rango o dominio de números IP.

La utilidad TELNET de INTERNET permite conociendo el número IP de otro ordenador conectado a la red lanzar una ventana de conexión directa hacia dicho ordenador que nos colocaría en la "puerta de entrada" del otro ordenador.

Todas las utilidades de INTERNET pueden ser utilizadas una vez conseguida la conexión desde el usuario al proveedor y su coste económico es muy bajo pues normalmente el usuario conecta vía módem con un proveedor que se encuentra en su

ciudad por lo que el coste de la conexión es el de una llamada local y son los proveedores los que corren con los gastos de las comunicaciones a nivel mundial.

INTERNET y en general la redes telemáticas constituyen un medio tecnológico cada vez más utilizado en el mundo estimándose que el número de usuarios de la red en el año 2.000 podría llegar a ser de 120 millones

Como tal medio no escapa al uso que de él realiza el mundo delincuencial en especial la denominada delincuencia de cuello blanco y también los grupos o bandas organizadas.

Surgen así determinadas figuras delictivas sobre todo en la década de los noventa donde el hecho destacable es la utilización por los autores materiales de medios informáticos y/o electrónicos destacando especialmente INTERNET ya que esta red abierta de baja seguridad técnica permite a estos delincuentes conseguir entre otros efectos un mayor anonimato e internacionalidad en sus actividades ilícitas.

Podríamos decir por tanto que el auge de los denominados "delitos informáticos" va íntimamente ligado al desarrollo en los años 90 de Internet y que no existe un concepto concreto de DELITO INFORMATICO pues no existen delitos informáticos propiamente dichos sino delitos ya existentes y reflejados en la legislación cometidos a través de medios informáticos y/o electrónicos.

2.- TIPOS DE "DELITOS INFORMÁTICOS" EN LA LEGISLACIÓN ESPAÑOLA.

2.1. - Delitos contra el orden socioeconómico. (Titulo XIII. Código Penal).

Articulado:

Art. 248 C.P.

1. *Cometen estafa los que, con ánimo de lucro utilizaren engaño suficiente para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo profesional.

El párrafo 2º del art. 248 se configura como delito de estafa tradicional el "fraude informático", sustituyendo el término de "engaño" por el de "manipulación"

La manipulación informática puede tener lugar a la entrada de datos (por acción u omisión) en el mismo programa y en la salida de datos. Como dice Bueno Arús (Actualidad Informática Aranzadi nº.11 11) la manipulación a distancia de los datos suscita el problema de la ley penal aplicable cuando no coincida la del lugar de manipulación con la del lugar donde se produce el resultado fraudulento.

Casuística:

-Generación aleatoria de números de tarjetas crédito que son aceptadas en operaciones bancarias.

- Utilización de SNIFFERS para obtener números de tarjetas de crédito y poder realizar transacciones en Entidades Bancarias que dan acceso a sus clientes a través de Internet. Caso CITIBANK 1994.

Articulado:

Art. 243. -

" El que con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión....."

Casuística:

- Extorsión a empresas.

Articulado:

.. Ley 19/93 de 28 de diciembre sobre determinados medios de prevención de Blanqueo de Capitales.

.. R.D. 925/95 de 9 de junio que desarrolla la Ley.

Casuística:

- *Blanqueo de Capitales. (Anonimato).*

Es posible encontrar en INTERNET determinados anuncios en páginas WEB desde proveedores ubicados en paraísos fiscales como Gibraltar o las Islas Caimán donde se ofrece la compra de bienes de gran importancia como son casas terrenos o empresas.

2.1.1. - Delitos relativos a la propiedad intelectual.

Articulado:

Art. 270 C.P.

" Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya, o comunique públicamente, en todo o en parte, una obre literaria artística, científica o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual".
" la misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización ".

" Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o neutralización de cualquier dispositivo técnico que haya sido utilizado para proteger programas de ordenador".

Casuística:

- La copia no autorizada de programas de ordenador (piratería) en la mayor parte de los casos a través de soporte CD-ROM constituye una agresión ilícita de los derechos de autor que generalmente se castiga por medio de estos artículos si bien el art. 272 del C.P. remite a La Ley 22/87 de la propiedad intelectual en materia de responsabilidad civil derivada del delito.

La casuística en nuestro país en relación a este tipo de delitos es ya histórica, pues tanto la Guardia Civil como el Cuerpo Nacional de Policía ha desarrollado a lo largo de la década de los 80 y 90 numerosas aprehensiones de CD,s conteniendo copias ilegales de programas informáticos.

Sin embargo podríamos decir que el auge de INTERNET ha dado lugar a la proliferación de este tipo de piratería informática a niveles casi "industriales" causando graves perjuicios económicos a las compañías dedicadas a la producción y comercialización de Software.

Un caso investigado por UCO (Unidad Central de Policía Judicial de la Guardia Civil) nos remite a un pequeño país de Centroamérica donde desde un ordenador ubicado en una Universidad se realizan copias maestras de CD,s que son ubicadas en un proveedor de EEUU (centro de distribución central) a través de Internet. Desde este punto una vez que se satisfacen determinadas cantidades de dinero a través de la red (normalmente pagos con tarjetas de crédito) se transfieren las copias a otros centros de distribución existentes en el Reino Unido, Alemania y España. Cada CD es comercializado finalmente a un precio de 5.000 pts y el valor real del software contenido en cada uno de ellos es aproximadamente de 500.000 ptas. Mensualmente aparece en la red una nueva versión del CD y la distribución estimada en España es de unos 100 CD,S diarios, las perdidas por tanto para las compañías productoras de Software serían aproximadamente de 4.000 millones de ptas. ya que la operación se realiza desde 1.990.

2.1.2. - Delitos de daños.

Articulado:

Art. 264. 2

" La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier medio dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"

Casuística:

Existen multitud de utilidades informáticas que pueden ser empleadas para dañar sistemas informáticos o redes telemáticas simplemente con la intención de causar un daño sin que exista una finalidad lucrativa o de extorsión. Los más comunes son:

- Bloqueo de ordenadores mediante "electronic mail bomb"

Existen determinados programas relacionados con la gestión de correo electrónico que permiten generar multitud de órdenes de correo desde un origen a un solo destinatario de tal forma que es posible bloquear el ordenador del destinatario generando una gran multitud de estas órdenes o mensajes.

- Introducción en sistemas informáticos de:

..Caballos de Troya.-

Es una forma de dañar datos de sistemas informáticos consistente en insertar determinadas instrucciones en la secuencia de ejecución de un programa de tal forma que realiza una función no autorizada e incluso daña otros datos mientras aparentemente realiza una función correcta.

Un caso especial dentro de los denominados Caballos de Troya son los denominados *Salamis* consistentes en pequeñas modificaciones en programas utilizados en banca que realizan pequeñísimos asientos en multitud de cuentas bancarias de forma que no sean detectados por su importancia y finalmente transferencias de esos asientos a otra cuenta bancaria.

..Virus.

Tiene similitudes con un virus biológico ya que un virus biológico necesita un cuerpo vivo para vivir, infecta células vivas de dicho cuerpo y se reproduce. En este sentido un virus informático es un programa informático que modifican a

otro programa dañándolo de tal forma que permite la nueva reproducción del programa o virus

.. *Worms (Tormentas).* -

Un "worm" o tormenta es un programa informático que no necesita otro para funcionar al igual que el virus. El worm simplemente se duplica el mismo tantas veces como está programado hasta que desborda por tamaño el ordenador o sistema informático donde esta instalado.

..*Bombas Lógicas.*-

Es un programa introducido en un sistema informático que se activa al coincidir una fecha y hora contenida en dicho programa con el reloj del ordenador donde se encuentra instalando, desencadenando a partir de ese momento una serie de ordenes (normalmente borrado físico de información) que dañan el sistema. Una bomba lógica puede ser introducida varios años antes de actual.

- *Destrucción de equipo informático (Datos, Software o Hardware).*

2.2. - Delitos relacionados con la Libertad Sexual (Título VIII C.P.).

Articulado:

Art. 186 C.P.

" El que por cualquier medio directo, difundiere, vendiere, o exhibiere material pornográfico entre menores de edad o incapaces, será castigado con la pena de multa de tres a diez meses."

Art. 187.1 C.P.

" El que induzca, promueva, favorezca o facilite la prostitución de una persona menor de edad o incapaz, será

castigado con las penas de prisión de uno a cuatro años y multa de doce a 24 meses."

Art. 189.1 C.P.

" El que utilizare a un menor de edad o a un incapaz con fines o en espectáculos exhibicionistas o pornográficos será castigado con la pena de prisión de uno a tres años."

Casuística:

- Pornografía infantil.

En este caso INTERNET es una vez más el medio informático utilizado para cometer un delito ya recogido en el código penal y cometido a través de otros medios como pueden ser revistas especializadas que se venden en sex-shops o círculos cerrados.

La primera cuestión planteada es si INTERNET puede considerarse "un medio directo" de difusión de pornografía entre menores de edad. Bien es sabido que son muchos los menores de edad que pueden acceder a través de INTERNET a este material pornográfico sin embargo en este caso no parece que hasta ahora la jurisprudencia en nuestro país considere al medio informático como un medio a tener en cuenta según los condicionantes en el artículo 186 del C.P.

La segunda cuestión planteada es el submundo delincuencial existente detrás de la publicación de pornografía infantil en INTERNET.

Sobre todo en las NEWS o foros de debate en INTERNET podemos encontrar numerosas fotografías y videos

pornográficos que son mostrados o comercializados (pagos a través de medios de pago electrónicos) al resto de los usuarios de la red desde proveedores existentes en España y otras partes del mundo.

La problemática se plantea cuando las imágenes presentadas en esos foros de debate son imágenes reales de menores de edad en las cuales puede detectares practicas sexuales abusivas e ilegales e incluso se ofrecen contactos con esos menores para lo cual es preciso abonar cierta cantidad de dinero y ponerse en contacto con el pederasta o pedófilo a través de una dirección de correo electrónico

Esta problemática crece cuando dichas practicas son realizadas por ejemplo en algún lugar de España. El presunto pedófilo "coloca" para

comercializarlas las imágenes pornográficas con menores de edad en un proveedor de EEUU donde es libre y gratuito acceder para publicar cualquier tipo de información sin que sea registrada la identidad de la persona que origina la información

Ante este ejemplo la pregunta es ¿Dónde realmente se comete el delito de pornografía infantil?. ¿Cómo es posible detectar el origen si no existe un registro fidedigno de quien ha colocado la información en el proveedor?.

2.3. - Delitos relacionados con el orden Público. (Título XXII C.P.).

Articulado:

Art. 18 C.P.

" 1. La provocación existe cuando directamente se incita por medio de la imprenta, la radiodifusión o cualquier otro medio de

eficacia semejante, que facilite la publicidad ante una concurrencia de personas, a la perpetración de un delito.

Es apología a los efectos de este Código, la exposición, ante una concurrencia de personas o por cualquier medio de difusión,

de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.....

Art. 571 C.P.

" Los que perteneciendo, actuando al servicio o colaborando con bandas armadas, organizaciones o grupos cuya finalidad sea la de subvertir el orden constitucional o alterar gravemente la paz pública, cometan los delitos de estragos o de incendios tipificados en los artículos 346 y 351 respectivamente, serán castigados con la pena de prisión de 15 a 20 años....."

Casuística:

Podemos considerar a los grupos terroristas como el ejemplo de delincuencia organizada más desarrollado y peligroso existente en nuestros idas.

No es extraño por tanto que también hayan utilizado loes medios informáticos y concretamente INTERNET para desarrollar sus actividades.

- Atentados a Sistemas Informáticos de centros neurálgicos del Estado, como Aeropuertos, Empresas de Electricidad de ámbito estratégico, Sistema de impresión de billetes o Centrales Nucleares.

Este fue el caso de las Brigadas Rojas en Italia en los años 70 ya que atentaron contra más de 25 centros considerados de interés neurálgico para el Estado

- Utilización de correo electrónico (e-mail) asociado a encriptación de datos en PGP.

Otro ejemplo de utilización de estos medios para subvertir el orden público puede ubicarse en la red de comunicación de algunos de estos grupos.

Es fácil transmitir cualquier tipo de información de interés para un grupo terrorista (ordenes de ejecución de un atentado documentos, planos, libros, fotografías de objetivos, videos, etc.) a través de correo electrónico entre dos usuarios conectados a

INTERNET, uno por ejemplo en España y otro en Francia o Bélgica y todo ello sin moverse de casa.

También existen posibilidades técnicas de interceptar este tipo de mensajes e identificar origen y destino real de la información sin embargo las dificultades aumentan cuando el contenido del mensaje es encriptado mediante alguna clave.

En este sentido es preciso destacar que la mayoría de los buenos sistemas de encriptación eran coto cerrado para las agencias o centro de inteligencia de determinados piases sin embargo hoy en día es relativamente fácil para cualquier usuario encontrar y disponer en INTERNET de un sistema de encriptación de datos de usuario como PGP (Pretty Good Privacy) de equiparable eficacia a los grandes sistemas de encriptación conocidos.

Como ejemplo de la utilización de este tipo de encriptación en mensajes transmitidos por correo electrónico entre diversas células de un grupo terrorista podemos destacar el uso de este sistema por el grupo Neonazi que realizó el Atentado en los Juegos Olímpicos de Atlanta en 1.996.

- Presentación de información sensible en INTERNET.

Es relativamente fácil encontrar información en INTERNET sobre el frente armado del IRA (Irish Republic Army) o del frente de Masas de ETA también llamado colectivo KAS (Koordinadora Abertzale Socialista) o sobre grupos neonazis o sectas que dan publicidad a través de la red de sus actividades ilegales y animan a contactar con este tipo de organizaciones a través de correo electrónico. ¿Podríamos considerar que estamos ante un caso de apología o provocación recogidos en el artículo 18 del C.P.? . Son preguntas que la doctrina y la Jurisprudencia deberá ir despejando en los próximos años.

2.4. - Delitos contra la Intimidad (Título X C.P.).

2.4.1- Revelación de Secretos.

Articulado:

Art. 197.

1. El que para descubrir los secretos o vulnerar su intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes o de correo electrónico, o cualquiera otros documentos o efectos personales o intercepte sus comunicaciones o utilice artificios técnicos de escucha, transmisión grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice, o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

Iguales penas se impondrán al que sin estar autorizado acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros se impondrá la pena de....."

5. Igualmente cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual o la víctima fuera un menor de edad o un incapaz se impondrán las penas....."

6. *Si los hechos se realizan con fines lucrativos se impondrán penas..."*

Casuística:

-Obtención de secretos teóricamente eliminados. Caso T.Col. Oliver North en Iran-Contra.

-Interceptación de líneas de datos y Captura de emanaciones electrónicas.

-Utilización de "Back Doors". Modificación en un programa que permite traspasar la seguridad

-Uso de Palabras de paso de otras personas.

-Uso de Scanners (Demon Dialers programs). Caso Ardita Argentina 1.994

-Utilización de Sniffers - Hackers. Caso Guardia Civil en Tarragona 1.9973. -

EJEMPLOS DE DIVERSA LEGISLACIÓN PENAL Y PROCESAL SOBRE "DELITOS INFORMÁTICOS" EN EL MUNDO.

EE.UU.- LEY CRIMINAL FEDERAL.

Título 15- Comercio.

Capítulo 41. - Protección del consumidor de crédito.

Sec. 1644. Uso fraudulento de tarjetas de crédito.

A) Uso, tentativa o conspiración de uso de una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida en transacciones comerciales interestatales o que afecten al comercio exterior.

B) Transporte, tentativa o conspiración de uso de una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida en transacciones comerciales interestatales.

C) Uso del comercio interestatal para vender o transportar una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida.

D) Recepciones, uso y transporte en el ámbito interestatal con conocimiento, de bienes obtenidos mediante el uso de una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida.

E) Uso de tickets en el ámbito interestatal y con conocimiento de su origen fraudulento obtenidos el uso de una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida.

F) Obtención de bienes, servicios o dinero procedentes del uso de una tarjeta ficticia, alterada, manipulada, robada, perdida o fraudulentamente obtenida.

Título 17- Propiedad Intelectual.

Capítulo 5. - Infracción de los derechos de Autor.

Titulo 18. - Crímenes y procedimientos.

Capítulo 5. - Daños

Sec. 81. - Daños a medios informáticos y/o electrónicos dentro de jurisdicción especial marítima y territorial.

Capítulo 31. - Sustracción y Robo.

Sec. 641. - Dinero Público, propiedad o registros. Obtención fraudulenta y/o sustracción a través de cualquier medio (incluido el informático y/o electrónico) de dinero público.

Capítulo 37. - Espionaje.

Sec793.- Observación, transmisión ilegal o perdida de información relacionada con defensa.
Sec. 794. - Observación y Obtención ilegal de información relacionada con la defensa para ayudar a un gobierno extranjero.

Capítulo 47. - Fraude y falsificaciones.

Sec. 1001. - realización a través de cualquier dispositivo incluido el informático y/o electrónico de falsificaciones (de billetes, documentos, etc.)
Sec. 1029. - Fraudes y actividades relacionadas con relación a dispositivos de acceso (redes informáticas, ordenadores, cajeros, etc.).

Capítulo 63. - Fraude de correo.

Sec. 1341. Fraudes a través del uso de correo (postal y/o electrónico).
Sec. 1343, Fraudes a través de cable, radio o televisión.

Capítulo 65. - Ataques maliciosos

Sec. 1361. - Ataques maliciosos a la propiedad del Gobierno o sus departamentos y agencias (infraestructuras y medios informáticos, etc.).

Capítulo 101. - Registros e Informes.

Sec. 2071. - Sustracción, mutilación o destrucción así como tentativa de informes y registros propiedad del Gobierno de EEUU.

Capítulo 105. - Sabotaje.

Sec. 2155. - destrucción o alteración maliciosa de materiales, dispositivos y utilidades relativos a la defensa Nacional

Capítulo 113. - Sustracción de Propiedad.

Sec. 2314 Transporte, transmisión o transferencia ilegal a través de cualquier medio (incluido el electrónico y/o informático) de dinero, objetos robados u obtenidos fraudulentamente, sellos de tasas del estado, etc.

Capítulo 119. - Interceptación ilegal de comunicaciones por cable y/ electrónicas así como comunicaciones orales.

Capítulo 206. - Prohibición del uso de dispositivos de seguimiento y observación de señales electrónicas (incluidas comunicaciones entre ordenadores) excepto en los casos previstos en la Ley (Autorizados por Fiscal para investigación policial).

Título 42. - Salud Pública y Privacidad.

Capítulo 21A. -

Seca 2000aa.Protección de la Privacidad.

Prohibición de acceso no autorizado a información reservada en medios informáticos

Ley Pública 103-414 sobre Asistencia en Comunicaciones.

Título I.- Interceptación ilegal de señales digitales.

Los siguientes Estados de EEUU tienen legislaciones específicas sobre delincuencia informática:

-Alabama:	Título 13a de la Ley Criminal. De Alabama. Acta 13a-8-100.
-Alaska:	Título 11 de la Ley Criminal de Alaska
-Arizona:	Titulo 13 del Código Criminal de Arizona.
-Arkansas:	Título 5 de legislación sobre ofensas criminales.
-California:	Título 13 de Acta criminal de California. Sec. 1230.048
-Colorado:	Titulo 18 del Código Criminal de Colorado. Art. 5.5. Delitos informáticos.
-Conectica:	Título 53A del Código penal del Estado.
-Delaware:	Título 11 de la Ley Penal y de Procedimientos Penales.
-Florida:	Título XLVI. Capítulo 815. Delitos Informáticos
-Georgia:	Título 16 Crímenes y Ofensas de la Ley Criminal del Estado.
-Hawai:	División 5 del Código Penal de Hawai.
-Idaho:	Titulo 18 de la Ley Penal.Capítulo 22 sobre Delitos Informáticos.

-Illionois:	Cap. 38 de la Ley Penal del Estado.
-Indiana:	Título 35 de la Ley Penal y Procedimiento Criminal.
-Iowa:	Título XXXV de la Ley criminal. Cp. 716A Delitos Informáticos.
-Kansas:	Cap. 21 del Legislación Penal del Estado.
-Kentucky:	Título XI. Cap. 434 de la Ley Penal del Estado.
-Louisiana:	Título 14 de la Ley Criminal del Estado.
-Maine:	Título 17-A del Código Penal Principal.
-Maryland:	Art. 27 de la Ley Penal del Estado.
-Masach. :	Capítulo 233 del Estatuto del Estado.
-Michigan:	Capitulo 752 del Estatuto del Estado.
-Minnesota:	Capítulo 609 del Código Criminal del Estado.
-Mississippi:	Título 97. Cap. 45 Delitos Informáticos del Estatuto del Estado.
-Missouri:	Título XXXVIII del Estatuto del Estado.
-Montana:	Título 45 del Estatuto del Estado
-Nebraska:	Capítulo 28 del Estatuto del Estado
-Nevada:	Título 15 del Estatuto del Estado
-N.Hamp:	Título LXII del Código Criminal.
-N. Jersey:	Título 2A de la Ley de Administración de Justicia Criminal y Civil.
-N. México:	Capítulo 15 del Estatuto del Estado
-New York:	Título J del Estatuto del Estado
-N. Carolina:	Capítulo 14 de la Ley Criminal.
-N. Dakota:	Capítulo 12.1-06.1-08 del Estatuto del Estado
-Ohio:	Título XXIX de la Ley Procesal Criminal.
-Oklahoma:	Título 21 del Estatuto del Estado
-Oregon:	Título 16 del Estatuto del Estado
-Pensylvania:	Título 18 del Estatuto del Estado
-Rhode I. :	Título 11 del Estatuto del Estado
-S. Carolina:	Título 16 del Estatuto del Estado
-S. Dakota:	Título 43 del Estatuto del Estado
-Tennesse:	Título 39 parte 14 del Estatuto del Estado
-Texas:	Título 7. capítulo 33. - Delitos Informáticos del Estatuto del Estado
-Utah:	Título 76 del Código Criminal
-Vermont:	No cuenta con legislación sobre delincuencia informática.
-Virginia:	Título 18.2 del Estatuto del Estado
-Wash. :	Título 9a del Código criminal del Estatuto del Estado
-W.Virginia:	Capítulo 61 del acta de abusos y delitos informáticos
-Wisconsin:	Capítulo 943 del Estatuto del Estado
-Wyoming:	Título 6 del Estatuto del Estado

AUSTRALIA:

Acta 1914- parte vía de la Ley Criminal de Australia.

A) Sección 76a:

Se realizan en esta sección definiciones de terminología informática como:

- Ordenador con datos propiedad de la Commonwealth.

B) sección 76b:

- Acceso no autorizado y de forma intencionada a un ordenador con datos propiedad de la Commonwealth. (Pena prisión por 6 meses.)

- Con ánimo de defraudar y sin autoridad de acceder en un ordenador con datos propiedad de la Commonwealth.

- Acceso no autorizado a un ordenador que no es un ordenador de la Commonwealth pero relacionados con: (Pena prisión por 2 años).

.. La seguridad, la defensa y las relaciones internacionales de Australia.
.. Datos confidenciales relativos a procedimientos penales o civiles en Australia.

.. Datos referidos a la Seguridad Pública.
.. Datos privados de una persona.
.. Secretos comerciales.
.. Registros de una institución financiera.

.. Información comercial que ilegalmente utilizada puede producir ventajas comerciales en otras personas.

..

C) sección 76c:

- Destrucción, borrado o alteración intencionada de datos almacenados en un ordenador, o introducción de datos de forma no autorizada en un ordenador de la Commonwealth.
- Interferir, interrumpir o obstruir el uso legal de un ordenador de la Commonwealth (pena 10 años de prisión)

CANADA:

Código Criminal de Canadá:

A) Aquel que de forma fraudulenta y sin derecho:

- Obtiene directa o indirectamente cualquier servicio a través de un ordenador.
- Por medios electromagnéticos. Acústicos o mecánicos u otro dispositivo intercepta cualquier función de un ordenador.
-Introducción en un sistema informático con la intención de causar alguna de las ofensas contenidas en el Código Criminal.

B) Cometerá delito quien:

- Destruye o altera datos.
- realiza denegaciones de acceso a otras personas.

HOLANDA:

Acta de delitos informáticos de Holanda. Código Criminal.

- Art. 98. - Acceso no autorizado a secretos contenidos en un ordenador.

- Art. 138a. - Acceso no intencionado a los datos contenidos en su ordenador o en cualquier parte de su proceso.

- Art. 139a. - Uso de dispositivos técnicos que capten o graben las emanaciones de voz o señales digitales.

-Art. 139c- Uso no autorizado de un dispositivo técnico intencionadamente utilizado para interceptar, grabar datos transferidos a través de la infraestructura de comunicaciones.

-Art. 161. - Destrucción de datos, daños o denegaciones de servicio en sistemas automáticos usados para el almacenamiento de datos el proceso de datos en las telecomunicaciones.

-Art. 232. - Falsificaciones de cheques, tarjetas de crédito. Así como su uso.

- Art. 273. - Revelaciones de secretos contenidos en un ordenador por parte de al persona que tiene la obligación de preservarlos.

- Art. 317. - Extorsión a personas o empresas con la amenaza de destruir o alterar los datos contenidos en un sistema informático.

- Art. 326c. - Uso de dispositivos técnicos para usar un servicio ofrecido al público con relación a las telecomunicaciones con el ánimo de no pagar.

- Art. 350a. - Prohibición de intencionadamente e ilegalmente distribuya datos dentro de un ordenador con el ánimo de causar daño a través de su multiplicación.

- Art. 351. - Daños a datos contenidos en ordenadores que gestiones sistemas relacionados con sistemas de telecomunicaciones, diques de protección, suministros del gas y agua, defensa nacional, etc.

FRANCIA:

Ley nº. 90-1170 de 30 de diciembre de 1990, modificado por Decreto nº. 92-1358 de 28 de diciembre de 1.992.

Art. 28. - Definición de facilidades criptográficas en medios informáticos y definición de penas para aquéllos que realicen usos no autorizados y exportación de facilidades criptográficas a través de medios informáticos.

No se considera "facilidad criptográfica" la protección de programas con palabras de paso.

Ej. : en Francia constituye un delito el uso y transferencia de un fichero de ordenador encriptado en PGP a través de INTERNET.

GHANA:

Proposición de Ley sobre delitos informáticos de 1.981.

1. - Cualquier persona que con ánimo de defraudar:

- Altere, dañe, destruya o manipule datos contenidos en un ordenador.

- Obtenga por cualquier medio y de forma no autorizada, información contenida en un ordenador y utilice la misma en ventaja de otras persona.

- Use un ordenador para cometer otro delito.

2. - Un tribunal en Ghana tendrá jurisdicción en estos delitos cuando:

- El acusado estuvo en Ghana.

- El programa o los datos con relación a los cuales fue cometido el delito fue almacenado, o usado en un ordenador o redes de ordenadores en Ghana.

GRAN BRETAÑA:

Acta de delitos informáticos:

- Sec. 1. - Acceso no autorizado a materiales relacionados con un ordenador.
- Sec. 2. - Acceso no autorizado con la intención de cometer o facilitar una ofensa posterior.
- Sec. 3. - Modificación no autorizada de materiales relacionados con un ordenador.
- Sec. 4. - Jurisdicción de los Tribunales Nacionales para perseguir los delitos contenidos en el acta.
- Sec. 8. - Relevancia de la Ley Externa.
- Sec. 9. - Procedimientos en Inglaterra y Gales.
- Sec. 13- Procedimientos en Escocia.
- Sec. 14. - Ordenes de búsqueda por delitos contenidos en esta acta.
- Sec. 16. - Aplicación en Irlanda del Norte.

4. - CONCLUSIONES

- Que no existen "delitos informáticos" entendidos como tales sino delitos contenidos en la vigente legislación cometidos a través de medios informáticos.

- Que desde hace aproximadamente 4 años, Internet se ha convertido en una red informática mundial abierta a cualquier persona (40 millones de usuarios en 1.995) donde prácticamente es imposible controlar las actividades ilegales realizadas a través de ella, debido a la inexistencia de un sistema judicial o policial uniforme y conjunto que permita a nivel mundial una respuesta ágil a estos problemas.

.- El mundo Cibernético o Internet es una realidad actual y no una entelequia futurista y que la sociedad en general y los medios de comunicación en particular demandan esfuerzos multidisciplinares, pero especialmente valoran la existencia de cuerpos policiales y Autoridades Judiciales que sepan estar a la altura de los nuevos retos tecnológicos como en es en este caso la persecución de delitos cometidos a través de medios informáticos o telemáticos.

- Existen Grupos Organizados de Delincuentes que utilizan medios informáticos y especialmente INTERNET para lograr sus fines ilegales y que si se les quiere combatir es preciso especializar a los investigadores en este campo.

- Que es necesario tener cuerpos policiales nacionales o internacionales de prestigio y se deben crear unidades que cuenten con personal y medios especializados para combatir este tipo de delincuencia.

- Que en todo el mundo proliferan unidades policiales especializadas en Delincuencia Informática en el seno de sus estructuras, estando centralizadas a nivel nacional debido al elevado costo de su mantenimiento (equipos técnicos, preparación del personal etc.).

- Que toda Unidad policial que comienza su andadura en este tipo de investigaciones debería considera los siguientes puntos:

.. Reconocer las propias posibilidades de la Unidad que investiga.

.. Crear estrategias a corto y largo plazo.

.. Crear un enlace estrecho entre investigadores y las empresas e industrias dedicadas al mundo de la informática.

..Intentar hacer ver a Fiscales y Jueces objetivamente donde se encuentra la actividad delictiva.

..Establecer contactos a nivel internacional para poder responder mejor a los diferentes tipos de criminalidad debido a la mayor internacionalidad de este tipo de delincuencia.

Tercer Panel
"LA ADMINISTRACIÓN PÚBLICA Y EL MUNDO DIGITAL: DESAFIOS PARA EL FUTURO"