

Delitos informáticos y Derecho penal

Luis Azaola Calderón



Vanguardia en
Ciencias Penales

13892

INSTITUTO DE FORMACIÓN PROFESIONAL

2

Colección: Investigación y ciencias penales

LUIS AZAOLA CALDERÓN
Coordinador de investigación del Instituto de Formación Profesional y
doctorando por la Universidad Complutense de Madrid



Vanguardia en
Ciencias Penales

Instituto de Formación Profesional

Biblioteca

Delitos informáticos y Derecho penal



Donación de libro por:
Jose Arturo Cejudo Cortez



Vanguardia en
Ciencias Penales

CLASIFICACION 364.168
CUTTER A894d
EJEMPLAR _____
No. DE ADQ. 13892
FECHA 13-Oct-2010

© Luis Azaola Calderón

Armando Téllez Reyes
Av. Jardín N° 592, Col. Euzkadi, C.P. 02660
Del. Azcapotzalco, México D.F.
ubijus@gmail.com
(0155) 55564511
(0155) 53566888

ISBN: 978-607-00-2428-3

Dirección de Arte y Diseño:
ROLANDO L. BARTOLO MESÍAS

Reservados todos los derechos. Ni la totalidad ni parte de este libro puede reproducirse o transmitirse por ningún procedimiento electrónico ni mecánico, incluyendo fotocopia, grabación magnética o cualquier almacenamiento de información y sistema de recuperación, sin permiso expreso del editor.

2010

DIRECTORIO EDITORIAL

DR. MIGUEL ÁNGEL MANCERA ESPINOSA
Procurador General de Justicia del Distrito Federal

DR. MIGUEL ONTIVEROS ALONSO
Coordinador General del Instituto de Formación Profesional

LIC. CATALINA GONZÁLEZ RODRÍGUEZ
Directora Ejecutiva de Profesionalización y Desarrollo
del Servicio Público de Carrera del Instituto de Formación Profesional

LIC. FRANCISCO ROMÁN PÉREZ SOLÍS
Director Ejecutivo de Formación, Docencia y Control Interno
del Instituto de Formación Profesional

MTRO. GERARDO FLORES ARNAUD
Director de Desarrollo Profesional y
Coordinación Interinstitucional

MTRO. LUIS AZAOLA CALDERÓN
Coordinador de Investigación del Instituto
de Formación Profesional

LIC. ALEJANDRO ROJAS PRUNEDA
Asistente del Consejo para la Aplicación del Nuevo Modelo
de Policía de Investigación

Editor Responsable:
Miguel Ontiveros Alonso

Instituto de Formación Profesional
4ª y 5ª Cerrada de Av. Jardín sin número, Col. Ampliación
Cosmopolita, Del. Azcapotzalco, México D.F.
www.ifp.pgjdf.gob.mx
ifp@pgjdf.gob.mx
(0155) 5345-5900

Procuraduría General de Justicia del Distrito Federal
Calle General Gabriel Hernández N° 56, Col. Doctores,
Del. Cuauhtémoc, C.P. 06720, México, D.F.

© UBIJUS Editorial

Contenido

Introducción	XI
CAPÍTULO I	
El internet	1
CAPÍTULO II	
Delitos cometidos en internet.....	21
CAPÍTULO III	
Conductas ilícitas cometidas en internet	23
CAPÍTULO IV	
Sujeto activo	27
CAPÍTULO V	
Sujeto pasivo	39
CAPÍTULO VI	
Las amenazas de internet a la información	41
CAPÍTULO VII	
La criminalidad informática	45
CAPÍTULO VIII	
Nociones generales del delito.....	49

CAPÍTULO IX	
El delito informático	49
CAPÍTULO X	
Clasificaciones	55
CAPÍTULO XI	
Modalidades	61
CAPÍTULO XII	
Delitos informáticos en el código penal español	75
CAPÍTULO XIII	
Delitos informáticos en la legislación mexicana	75
Conclusiones	105

Introducción

En este trabajo trataremos de analizar y explicar los delitos que pueden ser cometidos por medio de la informática, los que podemos considerar como un aspecto negativo del desarrollo de ésta. Las computadoras, si se manejan dolosamente, pueden llegar a ser medios para infringir la ley, utilizando mecanismos muy sofisticados para la comisión de los delitos, siendo éstos muy difíciles de detectar.

Desde hace ya varios años, la mayoría de las sociedades se han venido enfrentando a una revolución que muchos llaman "revolución informática", que ha modificado el trabajo y las labores de las personas y lo ha ido simplificando o, en algunos casos, reemplazando con el uso de máquinas y computadoras.

Desde que se inventó el ordenador el mundo se enfrenta a continuos avances en el ámbito de la informática, las técnicas de tratamiento de información, avanzadas tecnologías de telecomunicaciones, aumento en las capacidades de almacenamiento y procesamiento de datos, etc. Hoy en día, las relaciones comerciales y la sociedad en general dependen de la eficiencia y seguridad de la tecnología de la información.

Provocado por la rápida evolución de los sistemas informáticos, y debido a la gran dependencia de las sociedades a éstos, a lo largo de la historia ha ido en aumento el número de personas que emplean sus conocimientos informáticos para lograr dar con diferentes maneras y fórmulas para poder acceder y crear nuevas tecnologías, para poder manejarlas a su antojo y, a su vez, para descubrir su sistema y poder

adquirir conocimientos del mismo, y así lograr un mejor entendimiento de los mismos y de las computadoras en general.

Asimismo, los continuos avances en los programas de ordenador, en las aplicaciones de la informática y en las técnicas de almacenamiento y procesamiento de datos, así como las modernas tecnologías de las telecomunicaciones, han traído a su vez muy diversos problemas relacionados con nuevas formas de comisión de ilícitos, que tratan de romper con las barreras de seguridad y funcionamiento de estas tecnologías.

La informática o, en general, el tratamiento automatizado de datos, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afectan a los intereses fundamentales de las personas, es decir, la informática se presenta como factor criminógeno, pues permite el acceso y el manejo de bases de datos, programas de cualquier género, en ocasiones de forma lesiva para intereses básicos de las personas y de la sociedad, siendo más costosa la averiguación del autor y la prueba de los hechos debido a la naturaleza del procedimiento informático.¹

De esta forma, a lo largo de los años han existido y existen, cada vez más, un elevado número de personas que se dedican a la comisión de delitos relacionados con sistemas de procesamiento y transferencia automática de datos, etc., conductas delictivas que, en términos generales, se conocen con el nombre de delitos informáticos.

La tecnología y la informática se han extendido prácticamente a todas las áreas de la vida, trayendo aparejado el riesgo de que cada vez la delincuencia informática será más peligrosa y diversa.

Asimismo, las computadoras cada día son más potentes y cuentan con mayores prestaciones, además de que debido a la gran dependencia de la sociedad a éstas, ha provocado que los equipos informáticos se encuentren al alcance de cualquier persona, traducándose en que estas tecnologías pueden ser usadas tanto por personas capaces de convertir estos avances en crecimiento y productividad, como por personas capaces de cometer las más diversas conductas ilícitas.

Del mismo modo, con el advenimiento de la era de la computación han surgido diversos apelativos que se emplean para designar a perso-

nas o grupos de ellas que se dedican a estas actividades ilícitas. Así, la comunidad informática ha difundido durante años, en los principales medios de comunicación, el uso del término "hacker" como definición de sujetos que se infiltran o juegan con sistemas informáticos.

Los medios de difusión periodísticos adoptaron el nombre de hacker para calificar a toda persona involucrada en actos que atentan contra el derecho a la intimidad, infracciones a la propiedad intelectual a través de la protección de los derechos de autor, seguridad en las redes, autores de virus, intrusos de servidores, falsedades, sabotajes informáticos, fraudes informáticos, amenazas, calumnias e injurias, pornografía infantil, etc.

A los hackers también se les conoce con la palabra pirata, este apelativo es atribuido a las personas que hacen uso del software creado por terceros, a través de copias obtenidas ilegalmente, vale decir, sin permiso o licencia del autor. Al software no original se le denomina "copia pirata".

A lo largo de este trabajo se definirá y diferenciará cada término y cada conducta relacionada con actividades ilícitas empleando medios informáticos, y la importancia y trascendencia de estas figuras en la comisión de hechos delictivos, que cada día son más tecnificados por lo que la legislación debe actualizarse para no quedar rezagada.

¹ Mata y Martín, Ricardo M., *Delincuencia informática y derecho penal*, Editorial Edisofer, Madrid, 2001, p. 17.

CAPÍTULO I

Internet

Internet² es el nombre que se le da a una red informática creada a partir de un proyecto del Departamento de Defensa de Estados Unidos llamado DARPA NET (Defense Advanced Research Project Network), iniciado en 1969 y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes de transmisión de paquetes de diferentes tipos capaces de resistir las condiciones de operación más difíciles, y continuar funcionando aun con la pérdida de una parte de la Red general (por ejemplo, en caso de guerra).

² El 24 de octubre de 1995, el FNC (Federal Networking Council, Consejo Federal de la Red) aceptó unánimemente una resolución definiendo el término Internet. La definición se elaboró de acuerdo con personas de las áreas de Internet y los derechos de propiedad intelectual. La resolución: "el FNC acuerda que lo siguiente refleja nuestra definición del término Internet. Internet hace referencia a un sistema global de información que (1) está relacionado lógicamente por un único espacio de direcciones global, basado en el protocolo de Internet (IP) o en sus extensiones; (2) es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP; y (3) emplea, provee o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas". <http://www.tsi.com.pe/historia9.htm>. Consultada el 12 de diciembre 2006.

1.1 Historia de Internet³

A finales de la década de 1950, en pleno apogeo de la Guerra Fría entre los Estados Unidos de América y la URSS, el Departamento de Defensa del primero comenzó a preocuparse por lo que podría ocurrir con el sistema de comunicación nacional si estallaba una guerra nuclear. Una de las armas más importantes en una guerra son las comunicaciones y es uno de los primeros objetivos que el enemigo intentaría destruir.

En 1962 un investigador del gobierno estadounidense, Paul Baran, presentó un proyecto que daba solución a la interrogante planteada por el Departamento de Defensa. En ese proyecto, Baran propuso un sistema de comunicaciones mediante computadoras conectadas en una red descentralizada. De manera que si uno o varios nodos importantes eran destruidos, los demás podían comunicarse entre sí, sin ningún inconveniente.

Este proyecto se discutió por varios años y, finalmente, en 1969 la Advanced Research Projects Agency (ARPA) del Pentágono creó la primera red de ordenadores que se llamó ARPAnet. En la primer etapa sólo había cuatro computadoras conectadas a ella, mismas que provenían de la Universidad de California en Los Ángeles (UCLA), del Instituto de Investigaciones de Stanford (SRI), de la Universidad de California en Santa Barbara (UCSB) y de la Universidad de Utah. Ya en 1971 se habían agregado once nodos más, y para 1972 había un total de 40 computadoras conectadas a la Red.

En 1972 y con la necesidad de establecer un protocolo de comunicación común entre todas las computadoras, que variaban en tipo y sistemas operativos (IBM y Unisys, por nombrar algunas), para que pudieran comunicarse entre sí, sin ningún inconveniente, se creó el InterNetworking Working Group.

En el año 1974 dos investigadores, Vint Cerf (Stanford University) y Robert Kahn (BBN), redactaron un memorándum titulado "A Protocol for Packet Network Internetworking", donde explicaban cómo podría resolverse el problema de comunicación entre los diferentes tipos de computadoras. Ocho años después, esta idea fue implementada en su totalidad (ya que en 1978 comenzó a utilizarse en algunas redes), y

³ <http://www.ontinyent.com/juanypaco/origenes.htm>. Consultada el 12 de diciembre 2006. http://www.uigv.edu.pe/facesc/ingsi/investig/historia_internet.htm. Consultada el 12 de diciembre 2006.

se le denominó Transmission Control Protocol-Internet Protocol (TCP-IP). A partir de aquí (1982) empezó a utilizarse la palabra Internet. Este protocolo fue adoptado inmediatamente como estándar por el Departamento de Defensa Estadounidense para su red de computadoras y también, en 1982, ese organismo decidió su separación de ARPAnet y la creación de una red propia llamada MILnet.

A mediados de la década de 1980, la National Science Foundation (NSF), decidió que era necesaria una red de trabajo de alto rendimiento para enlazar cinco centros que poseían superordenadores y así poder dar acceso a los investigadores que se encontraban en distintas ciudades de Estados Unidos. En 1987 el NSF crea la NSFnet, que conectaba siete Networks con los cinco centros de supercomputadoras antes mencionado. Con esta nueva Red, la velocidad de transferencia entre los distintos nodos se incrementó a 1.5 megabits por segundo. Hasta ese momento, la velocidad de transferencia, entre nodos, era de 56 kilobits por segundo.

En 1971 Ray Tomlinson envió el primer mensaje de correo electrónico. No se sabe exactamente lo que escribió en ese mensaje. Tomlinson tampoco lo recuerda. El segundo mensaje fue enviado a las computadoras que estaban conectadas a la red donde él realizaba las pruebas, y en el mismo anunció la creación del correo electrónico y la manera de enviar los mensajes a otros usuarios de la red, utilizando el signo @ después del nombre que el usuario utilizaba para conectarse a la red.

En 1990 dejó de funcionar la red de trabajo que dio origen a Internet: ARPAnet. En ese mismo año el mayor centro de Internet en Europa era el CERN (European High-Energy Particle Physics Lab.). En ese organismo, en el año 1992, Tim Berners Lee (en la actualidad director del World Wide Web Consortium) creó la World Wide Web utilizando tres nuevos recursos: HTML (Hypertext Markup Language), HTTP (Hypertext Transfer Protocol) y un programa cliente llamado Web Browser. Todo este trabajo se basó en un escrito de Ted Nelson de 1974, en donde por primera vez se habló de hipertexto y enlaces.

En 1993, en el National Center for Supercomputing Applications (NCSA), de la Universidad de Illinois, Mac Andreessen creó, junto con un grupo de estudiantes, un programa llamado Mosaic (Web Browser), el cual ganó fama rápidamente. Mac Andreessen, al poco tiempo, se alejó del NCSA y junto con Jim Clark fundó Netscape. Andreessen se alejaría de un lugar donde trabajaba prácticamente gratis para crear otro que le daría enormes cantidades de dinero. También en 1993 la

National Science Foundation creó INTERNIC (the Internet Network Information Center), una especie de centro administrativo para Internet. El trabajo fue asignado a tres empresas:

- 1) Servicios de información: provisto por General Atomics. Proveía acceso vía ftp, gopher, wais, e-mail y www para obtener información en todo lo relacionado a Internet.
- 2) Servicios de registro: provisto por Networks Solutions, Inc. Se encargaba de asignar las direcciones de Internet (Internet addresses, Domain Names).
- 3) Servicios de base de datos: provisto por AT&T. Su papel era proveer a la comunidad de Internet de un directorio de recursos.

La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del networking (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Instituto Tecnológico de Massachusetts (MIT), en agosto de 1962, en los cuales Licklider discute sobre su concepto de galactic network (red galáctica). Él concibió una red interconectada globalmente a través de la cual cada uno pudiera acceder desde cualquier lugar a datos y programas. En esencia, el concepto era muy parecido al actual Internet. Licklider fue el principal responsable del programa de investigación en computadoras de la DARPA⁴ desde octubre de 1962. Mientras trabajó en DARPA convenció a sus sucesores Ivan Sutherland, Bob Taylor y el investigador del MIT Lawrence G. Roberts de la importancia del concepto de trabajo en red.

En julio de 1961 Leonard Kleinrock publicó, desde el MIT, el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red.

El otro paso fundamental fue hacer dialogar a las computadoras entre sí. Para explorar este terreno, en 1965, Roberts conectó un

⁴ La Advanced Research Projects Agency (ARPA, Agencia de Proyectos de Investigación Avanzada) cambió su nombre a Defense Advanced Research Projects Agency (DARPA, Agencia de Proyectos de Investigación Avanzada para la Defensa) en 1971. Más tarde retomó su antigua denominación ARPA, en 1993, para volver a DARPA en 1996. Nosotros la llamaremos siempre con su nombre actual (DARPA).

ordenador TX2 en Massachusetts con un Q-32 en California, a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de ordenadores de área amplia jamás construida. El resultado del experimento fue la constatación de que las computadoras de tiempo compartido podían trabajar juntas correctamente, ejecutando programas y recuperando datos a discreción en la máquina remota, pero que el sistema telefónico de conmutación de circuitos era totalmente inadecuado para esta labor. La convicción de Kleinrock acerca de la necesidad de la conmutación de paquetes quedó pues confirmada.

A finales de 1966, Roberts se trasladó a la DARPA a desarrollar el concepto de red de computadoras y rápidamente confeccionó su plan para ARPANET, publicándolo en 1967. En la conferencia presentó el documento donde se exponía también un trabajo sobre el concepto de red de paquetes a cargo de Donald Davies y Roger Scantlebury del NPL. Scantlebury le habló a Roberts sobre su trabajo en el NPL, así como sobre el de Paul Baran y otros en RAND.

El grupo RAND había escrito un documento sobre redes de conmutación de paquetes para comunicación vocal segura en el ámbito militar en 1964. Ocurrió que los trabajos del MIT (1961-67), RAND (1962-65) y NPL (1964-67) habían discurrido en paralelo sin que los investigadores hubieran conocido el trabajo de los demás. La palabra packet (paquete) fue adoptada a partir del trabajo del NPL y la velocidad de la línea propuesta para ser usada en el diseño de ARPANET fue aumentada desde 2,4 Kbps hasta 50 Kbps.⁵

En agosto de 1968, después de que Roberts y la comunidad de la DARPA hubieran refinado la estructura global y las especificaciones de ARPANET, DARPA lanzó una convocatoria para el desarrollo de uno de sus componentes clave: los conmutadores de paquetes llamados interface message processors (IMP, procesadores de mensajes de interfaz). La convocatoria fue ganada en diciembre de 1968 por un grupo encabezado por Frank Heart, de Bolt Beranek y Newman (BBN). Así como el equipo

⁵ Fue a partir del estudio de RAND como se inició el rumor de que ARPANET era algo relacionado con la construcción de una red resistente a la guerra nuclear. En realidad, esto nunca fue cierto. Solamente el estudio de RAND sobre seguridad vocal tomaba en consideración la guerra nuclear. Sin embargo, el trabajo posterior en Internetting hizo énfasis en la robustez y capacidad de supervivencia, incluyendo la capacidad de resistir la pérdida de grandes porciones de las redes en uso.

de BBN trabajó en IMP con Bob Kahn tomando un papel principal en el diseño de la arquitectura de la ARPANET global, la topología de red y el aspecto económico fueron diseñados y optimizados por Roberts trabajando con Howard Frank y su equipo en la Network Analysis Corporation, y el sistema de medida de la Red fue preparado por el equipo de Kleinrock de la Universidad de California, en Los Ángeles.⁶

A causa del temprano desarrollo de la teoría de conmutación de paquetes de Kleinrock y su énfasis en el análisis, diseño y medición, su Network Measurement Center (Centro de Medidas de Red) en la UCLA fue seleccionado para ser el primer nodo de ARPANET. Todo ello ocurrió en septiembre de 1969, cuando BBN instaló el primer IMP en la UCLA y quedó conectado el primer ordenador host. El proyecto de Doug Engelbart denominado Augmentation of Human Intellect (Aumento del Intelecto Humano), que incluía NLS, un primitivo sistema hipertexto en el Instituto de Investigación de Standford (SRI), proporcionó un segundo nodo. El SRI patrocinó el Network Information Center, liderado por Elizabeth (Jake) Feinler, que desarrolló funciones tales como mantener tablas de nombres de host para la traducción de direcciones, así como un directorio de RFC (Request For Comments). Un mes más tarde, cuando el SRI fue conectado a ARPANET, el primer mensaje de host a host fue enviado desde el laboratorio de Leinrock al SRI.

Se añadieron dos nodos en la Universidad de California, Santa Bárbara, y en la Universidad de Utah. Estos dos últimos nodos incorporaron proyectos de visualización de aplicaciones, con Glen Culler y Burton Fried en la UCSB, investigando métodos para mostrar funciones matemáticas mediante el uso de "storage displays" para tratar con el problema de actualizar la Red, y Robert Taylor e Iván Sutherland en UTA, quienes investigaban métodos de representación en 3-D a través de la Red. Así, a finales de 1969, cuatro ordenadores host fueron conectadas conjuntamente a la ARPANET inicial y se hizo realidad una embrionaria Internet. Incluso en esta primitiva etapa, se debe reseñar que la investigación incorporó tanto el trabajo mediante la red ya existente como la mejora de la utilización de dicha red. Esta tradición continúa hasta el día de hoy.

⁶ Incluyendo entre otros a Vinton Cerf, Steve Crocker y Jon Postel. Más tarde se unieron a ellos David Crocker, quien jugó un papel importante en la documentación de los protocolos de correo electrónico y Robert Bramen, quien desarrolló el primer NCP y después TCP para grandes ordenadores IBM y también jugó un papel a largo plazo en el ICCB y el IAB.

Se siguieron conectando ordenadores rápidamente a la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red. En diciembre de 1970 el Network Working Group (NWG) liderado por S. Crocker acabó el protocolo host a host inicial para ARPANET, llamado Network Control Protocol (NCP, protocolo de control de red). Cuando en los nodos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones.

En octubre de 1972, Kahn organizó una gran y muy exitosa demostración de ARPANET en la International Computer Communication Conference. Esta fue la primera demostración pública de la nueva tecnología de Red. Fue también en 1972 cuando se introdujo la primera aplicación "estrella": el correo electrónico. En marzo, Ray Tomlinson, de BBN, escribió el software básico de envío-recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo de coordinación. En julio, Roberts expandió su valor añadido escribiendo el primer programa de utilidad de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. Desde entonces, la aplicación de correo electrónico se convirtió en la mayor de la Red durante más de una década. Fue precursora del tipo de actividad que observamos hoy día en la World Wide Web, es decir, del enorme crecimiento de todas las formas de tráfico persona a persona que caracteriza a esta gran Red.

1.2 Las "autoridades" en Internet

Por extraño que parezca no hay una autoridad central que controle el funcionamiento de la Red, aunque existen grupos y organizaciones que se dedican a organizar de alguna forma el tráfico en ella.

Después de que las funciones militares de la Red se separaron en una subred de Internet, la tarea de coordinar su desarrollo recayó en varios grupos, uno de ellos la National Science Foundation que promovió bastante el uso de la Red, ya que se encargó de conectar cinco centros de súper cómputo que podían ser accesados desde cualquier nodo de la misma. Eso funcionó bien al principio, pero pronto fueron superadas las cargas de tráfico previstas, entonces se dio la concesión a Merit Network Inc. para que administrara y actualizara la Red, mejorándose las líneas de comunicación y dando un servicio mucho más

rápido, aunque este proceso de mejora nunca termina debido a la creciente demanda de los servicios.

El grupo de mayor autoridad sobre el desarrollo de la Red es la Internet Society, creada en 1990 y formada por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global a través de la tecnología de Internet. Puede decirse que esta sociedad es como un consejo de ancianos que tiene la responsabilidad de la administración técnica y dirección de Internet. Pero no es el único grupo que puede tomar decisiones importantes, existen otros tres grupos que tienen un rol significativo: el Internet Architecture Board (IAB), que toma las decisiones acerca de los estándares de comunicaciones entre las diferentes plataformas para que puedan interactuar máquinas de diferentes fabricantes sin problemas; este grupo es responsable de cómo se deben asignar las direcciones y otros recursos en la Red, aunque no son ellos quienes se encargan de hacer estas asignaciones, para eso existe otra organización llamada NIC (Network Information Center) administrada por el Departamento de Defensa de los Estados Unidos. El otro grupo importante es el Internet Engineering Task Force (IETF), en el cual los usuarios de Internet expresan sus opiniones sobre cómo se deben implementar soluciones para problemas operacionales y cómo deben de cooperar las redes para lograrlo. La dirección de Internet es, de cierta manera, una autocracia que funciona.

El enorme crecimiento de Internet se debe, en parte, a que es una Red basada en fondos gubernamentales de cada país que forma parte de Internet, lo que proporciona un servicio prácticamente gratuito. A principios de 1994 comenzó a darse un crecimiento explosivo de las compañías con propósitos comerciales en Internet, dando así origen a una nueva etapa en el desarrollo de la Red.⁷

1.3 El funcionamiento de Internet⁸

Internet es un conjunto de redes locales conectadas entre sí a través de un ordenador especial por cada red, conocido como gateway. El gateway es un conjunto de hardware y software que conecta redes que utilizan protocolos de comunicación diferentes, o que transmite datos

⁷ <http://www.salvaje.chapingo.mx/internet/>. Consultada el 25 de diciembre 2006.

⁸ <http://www.ontinyent.com/juanypaco/internet.htm>. Consultada el 25 de diciembre del 2006.

por una Red entre dos aplicaciones no compatibles. El gateway cambia el formato de los datos, de manera que les pueda entender la aplicación que los recibe.

Las interconexiones entre gateways se efectúan a través de diversas vías de comunicación, entre las que figuran líneas telefónicas, fibras ópticas y enlaces por radio. Pueden añadirse redes adicionales conectando nuevas puertas. La información que debe enviarse a una máquina remota se etiqueta con la dirección computarizada de dicha máquina.

Los distintos tipos de servicio proporcionados por Internet utilizan diferentes formatos de dirección (Dirección de Internet). Uno de los formatos se conoce como decimal con puntos, por ejemplo, 123.45.67.89 (también conocidos como nombres de dominio). Otro describe el nombre del ordenador de destino y otras informaciones para el encaminamiento, por ejemplo, 'mayor.dia.fi.upm.es'. Las redes situadas fuera de Estados Unidos utilizan sufijos que indican el país, por ejemplo (.mx) para México o (.es) para España. Dentro de Estados Unidos, el sufijo anterior especifica el tipo de organización a que pertenece la Red informática en cuestión, que puede ser una institución educativa (.edu), un centro militar (.mil), una oficina del gobierno (.gov) o una organización sin ánimo de lucro (.org).

Una vez direccionada, la información sale de su red de origen a través de la puerta. De allí es encaminada de puerta en puerta hasta que llega a la red local que contiene la máquina de destino. Internet no tiene un control central, es decir, ningún ordenador individual que dirija el flujo de información. Esto diferencia a Internet y a los sistemas de redes semejantes de otro tipo de servicios informáticos de red como CompuServe, America Online o Microsoft Network. En consecuencia, en la Red las personas pueden poseer cualquier nacionalidad, inclinación religiosa, tipo de vida y ser identificados bajo una personalidad virtualmente construida e irreal.⁹ Por esto se afirma que Internet es el reino del anonimato.

Este hecho que podría parecer sin importancia es, por el contrario, totalmente relevante, dado que la sociedad entera y el orden jurídico se encuentran sustentados sobre la base de la persona, entendiendo a la misma como un ente conocido o cognoscible. Sin embargo, dado

⁹ Nunca podremos estar seguros sobre la identidad de la persona escondida detrás de su sobrenombre o nickname.

el anonimato en Internet, la persona y la personalidad se encuentran en serios problemas, pues la comunicación que se origina por medio del conocido chat en Internet es impersonal, porque la mayoría de las personas no se conocen físicamente sino a través de este medio de comunicación virtual.¹⁰

Por lo anterior, el sujeto activo de los delitos informáticos cometidos en la Red generalmente es difícil de identificar, sino es que imposible.

En primer lugar, porque las nuevas técnicas han supuesto la incorporación al mundo jurídico de un nuevo ámbito de regulación (los derechos u obligaciones consecuentes a la creación, distribución, uso del hardware y del software, a las bases de datos, a la contratación de servicios informáticos o a la transferencia electrónica de datos); y porque tales aparatos y técnicas han supuesto cambios revolucionarios en la manera de entender las relaciones jurídicas tradicionales.¹¹

Los sujetos de la Red

De Miguel establece cinco categorías para diferenciar a los sujetos en la Red¹²:

- a. Los operadores de telecomunicaciones. Disponen de la infraestructura que permite la transmisión de datos.¹³
- b. Los proveedores de acceso a Internet. Proporcionan el servicio de conexión a la Red.¹⁴
- c. Los proveedores de servicios de Internet. Servicios que son

¹⁰ En este sentido, Silva Sánchez J. M. señala que "los fenómenos de la globalización económica y la integración supranacional tienen un doble efecto sobre la delincuencia. [...] conductas tradicionalmente contempladas como delictivas, deban de dejar de serlo, pues lo contrario se convertiría en un obstáculo a las propias finalidades perseguidas con la globalización y la integración supranacional". Aproximación al Derecho Penal Contemporáneo. Bosch Editores, Barcelona, 1992, p. 69.

¹¹ De Miguel Asencio, Pedro, Derecho privado de Internet. Editorial Civitas, Madrid, 2000, p. 35 y ss.

¹² Ídem.

¹³ Esto quiere decir que la computadora del usuario se enlaza con un sistema conectado directa o indirectamente a Internet, por medio de un proveedor de acceso.

¹⁴ Por lo general, los proveedores no disponen de conexión directa con Internet, sino que la realizan a través de una de las grandes redes de acceso por medio de un operador telefónico.

ofrecidos, por ejemplo, el buzón de correo electrónico, elaboración de páginas web, etc.¹⁵

- d. Los suministradores de servicios en línea y suministradores de contenido. Los primeros proporcionan información a los abonados a sus sistemas, mientras que los segundos son los titulares de la información y los datos que constituyen los contenidos, normalmente de las páginas web.
- e. Los usuarios. Aquellos que utilizan la Red.

Las anteriores categorías no son las únicas debido a la constante evolución que sufre la Red; también resulta conveniente aclarar que los unos no existirían sin los otros, ya que existe una relación de dependencia entre las categorías antes mencionadas.

1.4 Concepto de información

El término información¹⁶ tiene su origen en la acción de informar o informarse.¹⁷ La palabra informar, a su vez, significa enterar, dar noticia de alguna cosa. La definición de la Real Academia de la Lengua Española es "enterar, dar noticia de algo"; sin embargo, dichos conceptos se han ampliado porque hoy en día se puede considerar como un interés social valioso.¹⁸

Actualmente la palabra "información" engloba cualquier dato en el sentido más genérico y amplio que se pueda utilizar, el cual a su vez puede ser propiedad de un particular, de un Estado o de la sociedad en general.

Es sumamente difícil y a veces imposible valorar o cuantificar el "precio de la información", debido a que la misma varía dependiendo de la forma y fondo de su contenido, así como del sujeto que la posea.

¹⁵ "Los sitios web –o conjuntos de páginas web– están integrados por una serie de elementos relacionados entre sí, muchos de los cuales son creaciones originales, de distintas categorías: textos, fotografías, logotipos, gráficos, imágenes, sonidos, videos, animaciones. Cabe señalar que estas páginas web son susceptibles de ser objeto de propiedad intelectual". De Miguel Asencio, Pedro. Derecho privado... op. cit. p. 211.

¹⁶ Acción de informar o informarse. Efecto de informar o informarse.

¹⁷ Enciclopedia Microsoft Encarta 2002.

¹⁸ Gutiérrez Francés, Mariluz. "Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa" en: Mazuelos Cuello, Julio (comp.). Derecho Penal Económico y de la Empresa. Editorial San Marcos, Lima, 1997, p. 383 y ss.

No obstante, a lo largo de la historia han existido numerosos acontecimientos que han determinado el curso de la humanidad debido a que algunas personas, en un momento dado, obtuvieron y aprovecharon distintos datos para lograr un fin determinado.

Es por esto que el hombre ha dado especial importancia a la codificación de la información, con el propósito de anular o entorpecer la divulgación de la misma.

Mazuelos Coello¹⁹ establece que la información codificada se erige en un valor cuantificable y fundamental para el desarrollo de las actividades de las empresas, en el marco de la globalización económica. El autor señala que en el futuro la criminalidad no operará mediante asaltos a las bóvedas de los bancos sino que recaerá sobre las bases de datos de las empresas, como pueden ser su cartera de clientes, sistemas de cobranza, contabilidad, balances, estrategia de mercado, desarrollo de tecnología, etc. No cabe duda que hoy en día la información constituye un bien de capital.²⁰

Actualmente las personas físicas y morales²¹ invierten cuantiosas sumas en desarrollar sistemas de información automatizados que les permitan producir información para atender sus requerimientos organizacionales y, en consecuencia, intercambiar y manipular la más amplia variedad de datos, de diversa índole y con diferentes finalidades.²² Por tanto, si la información es nominativa o relacionada con las personas, al violentarla se atentaría contra la intimidad; de ser económica o representar valores, al utilizarla indebidamente se atentaría contra la propiedad o el patrimonio.²³

Como se apuntó en líneas anteriores, el valor de la información es plenamente subjetivo, por lo cual se ha optado por darle un valor desde un plano individual, por el titular de la misma, de ahí que se trate de un bien jurídico individual, personal.

¹⁹ Mazuelos Coello, Julio. "Protección jurídico penal de la información como valor económico de la empresa". En Revista Legal del Estudio Muñiz, Forsyth, Ramírez, Pérez-Taimán y Luna-Victoria Abogados, marzo de 1999, p. 38.

²⁰ Jijena Leiva, R., La protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile, Santiago, 2000, p. 149.

²¹ Incluyendo en las mismas a los Estados.

²² En <http://comunidad.derecho.org/congreso/ponencia29.html>. Consultada el 12 de Enero del 2005.

²³ Jijena Leiva, R., La protección penal... op. cit. p. 93.

1.5 Concepto de delito informático

Antes de entrar al estudio del delito informático o de lo que se entiende por éste, es importante mencionar que el, por ejemplo, el Código Penal español no emplea a lo largo de su articulado la expresión o el término de "delitos informáticos", de esta manera, hay que reconocer que estos ilícitos no existen desde un punto de vista jurídico-positivo, pero para efectos de este trabajo utilizaremos los términos de "delito informático" y/o "criminalidad informática" y/o "delincuencia informática".

Asimismo, un elemento importante a considerar es que, muchas veces, el delito se va a convertir en un "caso internacional", ya que la información viaja sin tener en cuenta las fronteras de los Estados.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado, a su vez, la necesidad de regulación por parte del derecho.

El delito informático se debe a la idea de que todos los programas de informática pueden ser vulnerados; asimismo, todos los sistemas de seguridad basados en el software son vulnerables. Por esto, las conductas que se pueden desplegar son innumerables, resultando necesaria una delimitación terminológica y conceptual de los llamados delitos informáticos.

Sin embargo, esta delimitación no es nada sencilla y, por el contrario, como señala Romeo Casabona,²⁴ las nuevas tecnologías informáticas deben ser reducidas a sus justos términos. En efecto, no se debe entender que por el simple hecho de que en una conducta intervenga un elemento del ámbito informático o un medio electrónico ésta sea un delito informático. El primer problema es que no existe una definición sobre lo que es un delito informático, y, hasta el momento, pocos países han hecho el intento de definirlo.

²⁴ Romeo Casabona, C. M., Poder informático y seguridad jurídica, Fundesco, Madrid, 1997, p. 41, citado por Matellanes Rodríguez, Nuria. Algunas notas sobre las formas de delincuencia informática en el Código penal. Hacia un Derecho Penal sin fronteras. Colex, Madrid, 2000, p. 130.

En las diversas legislaciones encontramos términos como delitos informáticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadoras, delincuencia relacionada con los sistemas informáticos, etc.; denominaciones que se han creado con el fin de señalar conductas ilícitas en las que se emplean sistemas informáticos.

Para Bramont-Arias²⁵ no existe un concepto único sobre delito informático; "ello debido a que la delincuencia informática²⁶ se basa en una cantidad de conductas que son difíciles de agrupar en un solo significado". Un sector de la doctrina considera que se debe recurrir a las características de los sistemas informáticos. Así, en opinión de Matellanes,²⁷ el significado de delito informático comprende aquellas conductas que constituyen agresiones a las funciones de procesamiento, transmisión y ejecución de programas propios de sistemas informáticos; de esta manera, el significado de delito informático se verá considerablemente reducido y excluirá a aquellos delitos tradicionales que utilizan los medios informáticos para la comisión de algún ilícito penal.²⁸

Para Davara Rodríguez²⁹ no parece adecuado hablar de delito informático, ya que no existe como tal si atendemos a la necesidad de una

²⁵ En este sentido, Bramont-Arias, Luis Alberto. Código Penal Anotado. Editorial San Marcos, Lima, 1998, p. 58.

²⁶ Para Gómez Peral la delincuencia informática es un conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. Ver en http://www.publicaciones.derecho.org/redi/No._06_Enero_de_1999/cuervo. Consultada el 20 de enero de 2005.

²⁷ Matellanes Rodríguez señala que "lo realmente específico de la delincuencia informática lo constituyen las funciones de procesamiento, transmisión y ejecución de programas propios del ordenador, con independencia de que la manipulación de estas funciones sea el medio o el objeto de la agresión ilegítima. Con esto se elimina del ámbito de la delincuencia informática todas aquellas conductas que no afecten a alguna de las funciones citadas." Matellanes Rodríguez, Nuria, Algunas notas sobre las formas de delincuencia informática... op. cit. p. 131.

²⁸ La misma autora también apunta que: "la utilización de un sistema de detonación de explosivos que funciona por control remoto para causar la muerte de alguien; o la entrega de una suma de dinero para adquirir un equipo de informática personal por correo a una empresa que resulta ser inexistente, o el mismo hecho de las agresiones al soporte físico de los equipos de procesamiento, debe quedar fuera de la noción de delitos informáticos." *Ibidem*, p. 129.

²⁹ Sin embargo, distingue dentro de la manipulación mediante la informática dos vertientes diferentes: a) Acceso y manipulación de datos y b) manipulación de los programas. En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo. Consultada el 20 de enero de 2005.

tipificación en la legislación penal para que pueda existir un delito. Por ejemplo, el Código Penal español de 1995 no introduce el delito informático, ni admite que exista como tal, aunque sí acepta la expresión por conveniencia para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. Los llamados delitos informáticos no constituyen una nueva categoría delictiva sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la Nación.

En este sentido, podemos afirmar que el delito informático no constituye una categoría autónoma, sino sólo una categoría criminológica que contiene una gran cantidad de conductas delictivas relacionadas con las computadoras o más ampliamente con los sistemas informáticos.

Como dijimos anteriormente se ha tratado de encuadrar los delitos informáticos dentro de los delitos comunes como son: robo, hurto, fraudes, falsificaciones, estafa, sabotaje, etc., pero debemos analizar si las categorías tradicionales son adecuadas o no respecto a estas modalidades delictivas. Los delitos informáticos pueden ser cometidos contra cualquiera de los diversos componentes del sistema de computación: tanto contra los equipos, instalaciones y redes de comunicación, como contra los programas y datos existentes en la memoria del ordenador.

En algunos casos el ordenador y sus aplicaciones constituyen el objeto material del delito (sobre el que recae físicamente la conducta) y, en otros, es un mero instrumento para cometer conductas tipificadas como delitos. En este sentido la doctrina alemana define estos supuestos como "el conjunto de actos (punibles o dignos de incriminación) en los cuales el ordenador es el instrumento o el objeto de la comisión."³⁰

De la misma manera señala González Rus, "las formas de intervenir 'sobre' el ordenador o 'con' el ordenador para la realización de un delito son muchas, pudiendo afectar a todos los elementos del sistema y a todas las operaciones precisas para su funcionamiento".³¹

³⁰ Romeo Casabona, C.M., Poder Informático y Seguridad Jurídica, Editorial Fundesco, Madrid, 1987, p. 22.

³¹ González Rus, J.J., "Aproximaciones al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", Revista de la Facultad de Derecho de la Universidad Complutense, núm. 12, Madrid, 1986, p. 112.

La Organización para la Cooperación Económica y el Desarrollo (OCDE) da una definición elaborada por un grupo de expertos, (París, 1983), que es considerada como "abarcante" y define a los "delitos relacionados con las computadoras" (computer-related crimes), como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".³²

Como podemos ver ésta es una definición demasiado amplia y a la vez completa ya que abarca toda conducta no autorizada o no ética que tenga relación, en términos generales, con la informática.

De la misma manera, existe otra definición, desde mi punto de vista muy general, que menciona que el delito informático, "es toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas".³³

Para Goldstein, el delito informático se diferencia de los delitos ordinarios en dos aspectos esenciales: en primer lugar, el delincuente no tiene necesidad de estar presente en el lugar del delito para cometerlo; en segundo lugar, este tipo no conoce frontera alguna, pues cualquier empresa equipada con un ordenador que disponga de un enlace telefónico con el exterior puede ser víctima de un fraude informático.³⁴

Romeo Casabona opina que no puede hablarse de un "delito informático", sino de "una pluralidad de ellos en los que encontramos, como única nota común, su vinculación de alguna manera con las computadoras, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho (delictivo o merecedor de serlo) presenta siempre características semejantes".³⁵ Por su lado, el Departamento de Justicia Estadounidense, conceptuaba el delito informático como "cualquier acto ilegal en relación con el cual el

³² Sieber, Ulrich, "Documentación para una Aproximación al Delito Informático", en Mir Puig, Santiago (comp.), *Delincuencia informática*, Editorial PPU, Barcelona, 1992, p. 66.

³³ Definición que aparece en las conclusiones del Congreso celebrado en Zaragoza en el año 1989 sobre el "delito informático", Véase Mata y Martín, Ricardo M., *Delincuencia informática y derecho penal*, Editorial Edisofer, Madrid, 2001, p. 21.

³⁴ Cita en Alonso Pérez, Francisco, *Delitos contra el patrimonio y contra el orden socioeconómico. Aspectos penales y criminológicos*, Editorial Colex, Madrid, 2003, p. 53.

³⁵ Romeo Casabona, C.M., *Poder informático y seguridad...*, op. cit. p. 41.

conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución".³⁶

Asimismo, Sneyers define a los delitos informáticos como "todos aquellos que se relacionan directa o indirectamente con el medio informático (computadoras, mini computadoras, microcomputadoras, equipo de tratamiento de textos, redes de telecomunicaciones y otros equipos informáticos, software, ficheros de datos y bases de datos)".³⁷

Camacho Losa los define como:

[...] toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.³⁸

Davara Rodríguez los define como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".³⁹

Para Jijena Leiva es "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma".⁴⁰

Como hemos visto, todas las definiciones antes mencionadas coinciden en el aspecto de que estamos en presencia de acciones dolosas cometidas directa o indirectamente, sobre o a través de medios o sistemas informáticos.

Desde mi punto de vista, y derivado de todas las definiciones mencionadas, se puede concluir que podemos encontrar supuestos delictivos que recaen sobre objetos pertenecientes al mundo de la informática (alteración, destrucción, sustracción de programas, ma-

³⁶ Romeo Casabona, C.M., *Poder informático y seguridad...*, op. cit. p. 42.

³⁷ Sneyers, A., *El fraude y otros delitos informáticos*, T.G.P., Madrid, 1990, p. 31.

³⁸ Camacho Losa, L., *El delito informático*, Gráficas Cóndor, Madrid, 1987, p. 17.

³⁹ Davara Rodríguez, M.A., *Manual de Derecho Informático*, Editorial Aranzadi, Pamplona, 1997, p. 286.

⁴⁰ Jijena Leiva, R., *La protección penal...*, op. cit. p. 32

terial o datos almacenados), así como también nos podemos encontrar ante la comisión de delitos variados, tales como delitos contra la intimidad, contra el patrimonio, contra la seguridad nacional, etc., en los que la informática representa el instrumento o medio de comisión o de ejecución del hecho punible. Por tanto, considero que una definición común de delitos informáticos sería todo delito cometido mediante o a través de un sistema de computación y con el aprovechamiento de las características técnicas específicas de todo sistema o medio computacional.

Es importante señalar que González Rus por su parte, establece una demarcación del ámbito de la criminalidad informática, basada en los temas sobre los que, según él, recaían los comportamientos abusivos o ilícitos vinculados a la informática:

- Atentados y peligros para la intimidad que se derivan de la formación y explotación de bancos de datos personales.
- Uso abusivo de los equipos e instalaciones informáticas y, en particular, el llamado "hurto de tiempo", que tiene lugar cuando el ordenador es utilizado por una persona autorizada a usarlo de ordinario pero en interés propio.
- Introducción de datos o registros fraudulentos.
- Alteración o destrucción de informaciones o ficheros.
- Sustracción o divulgación de informaciones, ideas, proyectos, etc., contenidos en el ordenador.
- Transferencias fraudulentas de dinero, instrumentos de crédito, propiedades, etc., mediante la manipulación del ordenador que interviene en la gestión de operaciones financieras, bancarias, etc.
- Repercusión penal de la falsificación o alteración de los datos contenidos en el ordenador o de los informes generados por el mismo, especialmente en lo relativo a su consideración como documento y su validez probatoria.
- Violación, por parte de los encargados del proceso electrónico de datos, de la obligación específica del secreto informático.⁴¹

⁴¹ González Rus, J.J., Aproximaciones al tratamiento..., op. cit. pp. 107 y 108.

- Por lo que hace a las características de estos tipos de delitos tenemos que para el autor mexicano Julio Téllez Valdez los delitos informáticos contienen las siguientes características:
- Son conductas criminales de cuello blanco (white collar crime) en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales en cuanto a que, muchas veces, se realizan cuando el sujeto se halla trabajando. Son acciones de oportunidad ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan. Ofrecen posibilidades de tiempo y espacio ya que, en milésimas de segundo, y sin una necesaria presencia física, pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.⁴²

Por último, Sieber menciona que los delitos informáticos tienen las siguientes características:

- 1.- Permanencia y automatismo del hecho.
- 2.- Sumas de daños.
- 3.- Volúmenes y desarrollo futuro de la criminalidad informática. (Cifra negra).
- 4.- Dificultades de averiguación.⁴³

⁴² Téllez Valdés, J., Derecho informático. 2ª edición, Ed. Mc Graw Hill, México, 1996.

⁴³ Sieber, Ulrich, Criminalidad informática..., op. cit., pp. 29-33.

Capítulo 2

Delitos cometidos en internet

2.1 Delitos contra el hardware

Existen diversos delitos perpetrados contra la parte física del sistema de computación, contra la parte denominada "hardware" que comprende redes e instalaciones así como también, en un sentido algo más amplio, las redes de comunicación del sistema. En este género de actos subyace la idea de actos físicos violentos, de agresión, contra los elementos materiales del sistema computacional. Por ello, en esta categoría de delitos son frecuentes los daños a la propiedad, los atentados, los incendios provocados. Los equipos de computación son costosos, su destrucción total o parcial, así como su inutilización temporal, generan pérdidas por montos cuantiosos.

2.2 Delitos contra el software

Por otra parte, existen delitos perpetrados contra los programas, contra el llamado software del sistema computacional. Los programas representan un área valiosa desde el punto de vista financiero y fundamental operativamente hablando, ya que dichos programas representan las directrices, las instrucciones con las cuales el sistema procesará los diversos datos. De ahí que su destrucción total o parcial implique pérdidas financieras y operativas considerables.

2.3 Delitos contra la memoria del ordenador

Existen, finalmente, delitos perpetrados contra los datos que reposan en la memoria del ordenador. Estos actos contra las bases de datos atentan contra la fiabilidad, la memoria y la integridad del sistema informático; son además, en muchos casos, el instrumento o mecanismo para la comisión de delitos patrimoniales.

En otros casos pueden no tener una relevancia económica directa, aunque son esencialmente graves aquellas situaciones en la cuales una persona o grupo de personas irrumpen en un sistema informático, generalmente gubernamental y relacionado con la defensa nacional, para incorporar datos falsos y no autorizados, generando de esta manera gravísimas distorsiones, así como reacciones humanas que, a partir de la información suministrada al ordenador, pueden generar resultados desastrosos para los gobiernos y para la seguridad de un Estado.

CAPÍTULO III

Conductas ilícitas cometidas en internet

A lo largo de la "breve" historia de la informática, y más concretamente de las conductas ilícitas relacionadas con ésta, diversos autores han tratado de delimitar y clasificar estas conductas, en este orden de ideas tenemos que, como punto de partida, existen ciertos aspectos de los sistemas informáticos que han sido y son susceptibles de sufrir conductas ilícitas y sancionadas por los Códigos Penales, y así podemos decir que éstas son:

- Manipulación en la fase de entrada (input).
- Manipulación en la fase de programación.
- Manipulación en la fase de procesamiento de datos.
- Manipulación en la fase de salida de datos (output).

Los delitos informáticos han sido objeto de variadísimas clasificaciones, tomando en cuenta la mayoría de éstas, los siguientes aspectos:

- El perjuicio causado.
- El papel que el computador desempeñe en la realización del mismo.
- El modo de actuar.
- El tipo penal en que se encuadren.

- Clase de actividad que implique según los datos involucrados.

A continuación mencionaré algunas de las diversas clasificaciones que se han ido elaborando sobre los delitos informáticos.

Empezando por Sieber, tenemos que para éste, los delitos informáticos presentan las siguientes modalidades:

- 1.- Manipulaciones del Ordenador.
 - Manipulaciones del "input".
 - Manipulaciones del programa.
 - Manipulaciones de la consola.
 - Manipulaciones del "output".
 - Abusos especiales en tiempo compartido "Time-Sharing" y teleproceso.
- 2.- Espionaje informático y hurto de "software".
- 3.- Sabotaje informático.
- 4.- "Hurto de tiempo".
- 5.- Delitos económicos en general.⁴⁴

Corcoy Bidasolo y Joshi Jubert los clasifican en cuatro grupos:

- 1.- Manipulaciones.
- 2.- Espionaje.
- 3.- Sabotaje.
- 4.- Hurto de tiempo.⁴⁵

Por otro lado, Romeo Casabona diferencia cinco grupos:

- 1.- Manipulaciones de datos informatizados.
- 2.- Piratería o copia ilegal de programas.
- 3.- Espionaje Informático.

⁴⁴ Sieber, Ulrich, *Criminalidad Informática...*, op. cit., pp. 15-28.

⁴⁵ Corcoy Bidasolo, M. y Joshi Jubert, U., "Delitos contra el patrimonio cometidos por medios informáticos", *Revista Jurídica de Cataluña*, Núm. III, 1988, Barcelona, pp. 135 y ss.

- 4.- Sabotaje informático.
- 5.- Agresiones en el soporte material informático.⁴⁶

El autor Ruiz Vadillo establece como supuestos de delincuencia informática los siguientes:

- 1.- Entrada, alteración, borrado y/o supresión de datos y/o programas informáticos efectuados de manera consciente o intencional con la finalidad de llevar a cabo una transferencia ilegal de fondos o de otra cosa de valor o simplemente de realizar una falsedad, cualquiera que sea su finalidad, o de obstaculizar o dificultar el funcionamiento de un sistema informático o de telecomunicaciones, si se hace ilegalmente.
- 2.- La vulneración del derecho exclusivo del titular de su programa informático protegido por la Ley con el fin de explotarlo comercialmente, entendida esta última palabra en sentido muy amplio. Y en igual sentido la violación de dibujos, signos o diseños protegidos de un círculo creado para su explotación comercial.
- 3.- El acceso o la interceptación de un ordenador o de un sistema de telecomunicaciones hecho dolosamente, incluyendo el método de obtención por medios ilegítimos de los datos de un ordenador y su divulgación, bien se trate de datos personales o de un secreto comercial o industrial.⁴⁷

Para Davara Rodríguez los delitos informáticos se pueden clasificar en las siguientes modalidades:

- 1.- Manipulación en los datos o informaciones contenidas en los archivos o soportes físicos informáticos ajenos.
- 2.- Acceso a los datos y/o utilización de los mismos por quien no está autorizado a ello.
- 3.- Introducción de programas o rutinas en otras computadoras para destruir información, datos o programas.
- 4.- Utilización del ordenador y/o los programas de otra persona sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.

⁴⁶ Romeo Casabona, C.M., *Poder informático y seguridad...*, op. cit., p. 43.

⁴⁷ Ruiz Vadillo, E., *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad informática*, Poder Judicial, Núm. Especial IX, Madrid, 1989, p. 62.

- 5.- Utilización del ordenador con fines fraudulentos.
- 6.- Agresión a la "privacidad" mediante la utilización y procesamiento informático de datos personales con fin distinto al autorizado.⁴⁸

Asimismo Rovira del Canto establece una clasificación de los ilícitos informáticos y así diferencia cuatro grupos criminológicos:

- Infracciones a la intimidad.
- Ilícitos económicos.
- Ilícitos de comunicación por la emisión y difusión de contenidos ilegales y peligrosos.

Otros ilícitos informáticos.⁴⁹

- Por último, el autor mexicano Julio Téllez Valdés distingue dos grupos:
- Como instrumento o medio: se tiene a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.
- Como fin u objetivo: se enmarcan a las conductas criminógenas que van dirigidas en contra de las computadoras como método, medio o símbolo en la comisión del ilícito.⁵⁰

Tomando en cuenta todas las clasificaciones mencionadas, desde mi punto de vista una clasificación común podría ser la siguiente:

- 1.- Manipulaciones del ordenador (input, output o de programas).
- 2.- Espionaje informático.
- 3.- Robo de software (piratería).
- 4.- Sabotaje informático.
- 5.- Acceso no autorizado a sistemas de procesamiento de datos.
- 6.- Delitos económicos en general.

⁴⁸ Davara Rodríguez, M.A., Manual de Derecho Informático..., op. cit., p. 289.

⁴⁹ Rovira Del Canto, E., "Delincuencia informática y fraudes informáticos", Editorial Comares, Granada, 2002, pp. 127-128.

⁵⁰ Téllez Valdés, J., Derecho Informático..., op. cit., p. 106.

CAPÍTULO 4

Sujeto activo

Los sujetos activos tienen como características:

- Poseen importantes conocimientos de informática.
- Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema).

A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Las opiniones en cuanto a tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional o nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

Estos delitos se han calificado de "cuello blanco", porque generalmente el sujeto que comete el delito es una persona de cierto status socioeconómico.

Desde hace ya varios años, y a partir del surgimiento de la informática, al delincuente informático y a la delincuencia informática en general, se le ha catalogado como una criminalidad de la denominada

de "cuello blanco". Lo anterior, debido a que los estudios sobre la criminalidad informática venían orientados principalmente en sus manifestaciones en el ámbito económico patrimonial en donde, además, la doctrina encontraba un elemento común respecto al sujeto activo, el cual consistía en determinar que el sujeto activo de un delito informático poseía un alto nivel socioeconómico.

Frente a esta postura aparecen otras teorías que sostienen que para ser delincuente informático no es necesario pertenecer a un determinado nivel socioeconómico, sino que más bien se relaciona al delincuente informático con el ámbito de desarrollo laboral o profesional, en la empresa víctima del delito informático.

Así Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas, que tienen acceso a los sistemas informáticos y conocen sus debilidades, y mantiene que "se trata de personas que podríamos encuadrar en lo que coloquialmente denominamos gente del montón que, por azar, por diversión, o por investigación técnica han descubierto ciertas debilidades en el sistema que les pone en situación de poder aprovecharse de dicha circunstancia, y coyunturalmente se encuentran en una situación en la que, sin ser desesperada, no les vendría mal un puñado de dinero extra".⁵¹ Romeo Casabona, por su parte, mantenía que los autores suelen ser primarios u ocasionales, y que generalmente se trata de empleados de las empresas afectadas.⁵²

Asimismo Corcoy Bidasolo y Joshi Jubert llegan a diferenciar tres grupos de posibles autores:

- 1.- Los operadores, programadores u otros sujetos que acceden legítimamente a la elaboración del programa.
- 2.- Cualquier sujeto a través de las terminales públicas o interceptando las líneas de transmisión de datos a distancia.
- 3.- Los titulares legítimos del sistema.⁵³

⁵¹ Camacho Losa, L. *El delito informático*, Gráficas Cóndor, Madrid, 1987, pp. 83-84.

⁵² Romeo Casabona, C.M., *Poder informático y seguridad...*, op. cit., p. 36.

⁵³ Corcoy Bidasolo, M. y Joshi Jubert, U., "Delitos contra el patrimonio cometidos por medios informáticos", *Revista Jurídica de Cataluña*, Núm. III, 1988, Barcelona, pp. 137.

Por otro lado, Gutiérrez Francés difiere de estos puntos de vistas y sostiene que: "la mayor parte de los comportamientos delictivos se llevan a cabo por personas vinculadas de algún modo a las empresas: empleados de confianza, directivos, consejeros, técnicos, especialistas en programación, operadores, oficinistas y, en general, todo tipo de sujetos con acceso material a las instalaciones de la unidad central de procesamiento de datos".⁵⁴

Por su parte, Ruiz Vadillo sostiene que, "autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados".⁵⁵ Vives Antón y González Cussac, en Comentarios al Código Penal de 1995, en referencia al Art. 248.2 (Estafa Informática), afirman que, "sujeto activo pueden serlo tanto las personas legítimamente autorizadas para acceder y operar en el sistema (operadores, programadores u otros), como terceros no autorizados que accedan a las terminales públicas o privadas o interceptando las líneas de transmisión de datos a distancia".⁵⁶

Choclán Montalvo sostiene que, en el ámbito de la delincuencia informática, el delito se presenta como acción de autores ocasionales que no precisan conocimientos informáticos especialmente cualificados, e incluso por la intervención de jóvenes que por mero recreo o curiosidad intelectual, en concepto de hackers (manipuladores no autorizados de sistemas informáticos), penetran en el sistema informático produciendo perjuicios de importante consideración.⁵⁷

Por último, y desde mi punto de vista, las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y, generalmente por su situación laboral, se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

⁵⁴ Gutiérrez Francés, M. de la L. *Fraude informático y estafa...*, op. cit., p. 75.

⁵⁵ Ruiz Vadillo, E., *Tratamiento de la delincuencia informática...*, op. cit., p. 78.

⁵⁶ Vives Antón y González Cussac, *Comentarios al Código Penal de 1995*, Editorial Tirant lo Blanch, Valencia, 1996, p. 1238.

⁵⁷ Choclán Montalvo, J. A. "Fraude informático y estafa por computación", en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, p. 309.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos, y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

A estos sujetos se les llama de diferentes maneras, dependiendo siempre de cómo actúan y de qué conductas son las que realizan.

4.1 Hackers

Es un término en inglés con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y constituyen una muestra de la nueva faceta de la criminalidad: el delincuente silencioso o tecnológico.

Es aquel al que simplemente le gusta husmear por todas partes, llegar a comprender el funcionamiento de los sistemas informáticos, incluso llegar a conocerlos mejor que las propias personas que los crearon. Generalmente realiza esta actividad como un reto intelectual y su intención no es producir daños, simplemente descifrar y conocer los sistemas informáticos.

Un hacker es una persona muy interesada en el funcionamiento de los distintos sistemas operativos; por lo general suele tener mucho conocimiento en lenguajes de programación. Además conoce la mayoría de los agujeros de un sistema operativo o de los protocolos de Internet, y los que no conoce los busca, y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor.

Se puede decir que los hackers se mueven por fines de autorrealización y conocimiento, nunca provocan daños intencionados en las máquinas, y comparten su información de forma gratuita y desinteresada.

De esta manera, Morant Vidal señala que los hackers son personas jóvenes (de 15 a 25 años, generalmente) muy interesadas en el funcionamiento de sistemas operativos; curiosos a los que simplemente les gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quienes lo inventaron.⁵⁸

⁵⁸ Morant Vidal, J. Protección penal de la intimidad frente a las nuevas tecnologías, Editorial Práctica de Derecho, Valencia, 2003, pp. 43-44.

El término de hacker ha quedado limitado a los intrusos informáticos, es decir, a los que realizan actividades de hacking o de intrusismo informático, esto es, de acceso no autorizado a un aparato, sistema, o red informática.

Para Sieber las conductas de hacking consisten en "el acceso no autorizado a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipulatorias, fraudulentas, de espionaje, ni de sabotaje, sino sencillamente como paseo por placer no autorizado (joyriding) por el ordenador de otra empresa (hackito ergo sum)".⁵⁹

Morón Lerma define a las conductas de hacking como "al conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y a la utilización de los mismos sin autorización o más allá del autorizado".⁶⁰

Alfonso Laso, por su parte, sostiene que con el término hacker "se designa a la persona que utiliza determinadas técnicas para acceder sin la debida autorización a sistemas informáticos ajenos".⁶¹

Para Ruiz Marco el hacking "consiste en el acceso no autorizado a los sistemas o los datos registrados informáticamente, mediante la vulneración del password o de los sistemas de seguridad (cortafuegos) implantado por el titular del ordenador".⁶²

Por último, Orts Berenguer y Roig Torres señalan que "el término hacker, se utiliza para designar aquellas personas expertas en informática que entran en otras máquinas por razones exclusivamente educativas o de diversión mientras que los intrusos con intenciones criminales o vandálicas tendrían reservado el término cracker".⁶³

⁵⁹ Sieber, Ulrich, Criminalidad informática..., op. cit., p. 77

⁶⁰ Moron Lerma, Esther. Internet y Derecho Penal: hacking y otras conductas ilícitas en la Red, Editorial Aranzadi, Navarra 2002, 2ª edición, p. 51.

⁶¹ De Alfonso Laso, Daniel, "El hackerin blanco. Una conducta ¿punible o impune?", en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, p. 512.

⁶² Ruiz Marco, Francisco. Los delitos contra la intimidad, especial referencia a los ataques cometidos a través de la informática, Editorial Colex, Madrid, 2001, p. 26.

⁶³ Orts Berenguer, Enrique y Roig Torres, Margarita. Delitos informáticos y delitos comunes cometidos a través de la informática, Editorial Tirant lo Blanch, Valencia, 2001, pp. 177-178.

4.2 Crackers

Los crackers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas. A los crackers también se les conoce con el nombre de piratas informáticos; asimismo, los crackers o piratas informáticos tienen dos variantes:

El que penetra en un sistema informático y roba información o produce destrozos en el mismo.

El que se dedica a desproteger todo tipo de programas, tanto de versiones software para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anti-copia.

Un aspecto para diferenciar a un hacker de un cracker puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación y conoce los lenguajes, mientras que el segundo se basa en programas ya creados que puede adquirir, normalmente, vía Internet.

Otro aspecto diferenciador es que el interés de un cracker es destrozar o causar problemas al ordenador que hay al otro lado, no es constructivo como un hacker, que trata de "mejorar" la red dando a conocer sus incursiones y los fallos que ha encontrado.

Por su parte Moránt Vidal señala que los crackers son los piratas informáticos, personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas, pudiéndose apreciar dos variantes de los mismos:

- a) El que penetra en un sistema informático y roba información o provoca destrozos en el mismo.
- b) El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anticopia.⁶⁴

Para Ruiz Marco el término cracking consiste en la infracción del software comercial, consiguiendo la copia de cualquier obra cultural

⁶⁴ Morant Vidal, J. Protección penal de la Intimidad..., op. cit., p. 44.

o científica (cinematográfica, musical, programa de ordenador, etc.), generando perjuicios económicos a los autores y a las industrias que, en algunos casos, pueden poner en peligro a todo un sector económico y pueden cambiar las propias estructuras tradicionales de producción y distribución.⁶⁵

Para Rovira del Canto la inicial pretensión del cracker no es el mero logro de un acceso informático o telemático no autorizado, con o sin vulneración de medidas de seguridad informáticas, sino la específica vulneración, corrupción o quebranto de los programas informáticos en sí mismos. Esta inicial motivación va normalmente dirigida hacia dos áreas: a la vulneración de los derechos de la propiedad intelectual, esto es la copia de software comercial de forma ilícita e indebida en lo que viene a denominarse "piratería informática", bien al quebranto o causación de daños en dichos programas informáticos, lo que viene a denominarse "sabotaje informático", normalmente ante el borrado o destrucción de datos, o la implantación en los programas o sistemas de virus informáticos que los destruyan.⁶⁶

De la misma manera, Alfonso Laso afirma que éste es el auténtico pirata virtual, y sostiene que el cracker no es sino la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etc.⁶⁷

Asimismo, Morón Lerma señala que las conductas de cracking se caracterizan por eliminar o neutralizar los sistemas de protección de un sistema informático, ya sea de un programa o del propio sistema operativo de la máquina. Habitualmente se rompe la protección de un programa que impide su copia no autorizada o la de una aplicación shareware que impide su uso, pasada una determinada fecha. Este comportamiento se cifra en la copia sin consentimiento y, en su caso, posterior distribución ilegal de programas informáticos (denominados warez, esto es, programas comerciales que han sido sometidos a la acción de un crack), con vulneración de los derechos de autor.⁶⁸

Por último, Orts Berenguer y Roig Torres señalan que cracker es "el experto en la eliminación de las protecciones de una aplicación in-

⁶⁵ Ruiz Marco, F. Los delitos contra la intimidad, especial referencia a los ataques cometidos a través de la informática, Editorial Colex, Madrid, 2001, p. 25.

⁶⁶ Rovira del Canto, E., Delincuencia informática..., op. cit., pp. 110-111.

⁶⁷ De Alfonso Laso, D. El hackerin blanco..., op. cit., pp. 512-513.

⁶⁸ Morón Lerma, E. Internet y Derecho Penal..., op. cit., p. 40.

formática que impiden su copia no autorizada, o de las protecciones de una aplicación shareware que impiden su uso pasada una determinada fecha. El término cracker es utilizado también para definir a quien accede ilegalmente a un sistema informático ajeno, con fines vandálicos o dañinos. En este último sentido, se utiliza como sinónimo la expresión dark-side hacker (hacker de lado oscuro)".⁶⁹

4.3 Cyberpunk

El término cyberpunk o vándalos cibernéticos se refiere a las conductas tendientes a causar daños en toda el área vinculada a la informática, esto es, afectando a los datos, programas o soportes informáticos, fundamentalmente a través de Internet.

Rovira del Canto señala que:

[...] de las conductas de cracker ha derivado un término, el de cyberpunk o vándalos cibernéticos, que viene referido, con carácter limitado, a las conductas de causación de daños indiscriminados en toda el área vinculada a la informática, esto es, afectante a los datos, programas o soportes informáticos realizados a través de las redes informáticas y telemáticas, sin un interés propiamente de obtención de un beneficio económico, sino con el específico ánimo de destruir.⁷⁰

Morón Lerma señala que "las conductas de daños informáticos o de vandalismo electrónico se concretan en asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones sobre dichos sistemas o para modificar o destruir datos. Esto es, se trata de comportamientos preordenados por el ánimo de perturbar los sistemas informáticos o de destruir los datos que contienen".⁷¹

Ruiz Marco señala que el vandalismo informático consiste en la destrucción o causación de daños en los datos, programas o sistemas informáticos, mediante la introducción de "virus" con o sin vulneración de la llave de paso (password), el bloqueo de servidores (mediante los denominados "ataques de denegación de servicios"), etcétera.⁷²

⁶⁹ Orts Berenguer, E. y Roig Torres, M. Delitos informáticos y delitos comunes..., op. cit., p. 175.

⁷⁰ Rovira del Canto, E. Delincuencia informática..., op. cit., p. 111.

⁷¹ Moron Lerma, E. Internet y Derecho Penal..., op. cit., p. 41.

⁷² Ruiz Marco, F. Los delitos contra la intimidad..., op. cit., p. 25.

Por último, Orts Berenguer y Roig Torres señalan que se trata de un movimiento literario, estético e ideológico, caracterizado por la desconfianza frente a las posibilidades de control de la sociedad que ofrecen las nuevas tecnologías.⁷³

4.4 Phreaker

Es el especialista en telefonía (cracker de teléfono). Un phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles, puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general móviles o celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

Estas personas, en la actualidad, también poseen conocimientos de tarjetas de prepago ya que la telefonía celular las emplea habitualmente. Sin embargo, es en estos últimos tiempos cuando un buen phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta, y/o emplean la informática para su procesador de datos.

Asimismo, buscan burlar la protección de las redes públicas y corporativas de telefonía, con el declarado fin de poner a prueba conocimientos y habilidades (en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores.

Rovira del Canto señala que el término phreaker, "es utilizado para designar a los defraudadores de líneas telefónicas a través de redes informáticas o telemáticas, específicamente a través de Internet".⁷⁴ El phreaking es un método de conocimiento exhaustivo de un sistema telefónico o de comunicaciones, vinculado estrechamente al hacking, mediante la ejecución, desde un ordenador de un programa de tipo wardialer (sintonizador de guerra) que realiza llamadas a unos números determinados y emite un informe de los resultados; el objetivo del

⁷³ Orts Berenguer, E. y Roig Torres, M. Delitos informáticos y delitos comunes..., op. cit., p. 175.

⁷⁴ Rovira del Canto, E. Delincuencia informática..., op. cit., p. 112.

delincuente es obtener una conexión a Internet cargando el coste de la llamada al titular de la línea a través de una línea gratuita para quien llama, pero no para quien la recibe, que es quien corre con los gastos.

Orts Berenguer y Roig Torres definen el término phreaking, como el "conjunto de técnicas empleadas para craquear la red telefónica para, por ejemplo, poder realizar llamadas gratuitas a larga distancia".⁷⁵

Para Moránt Vidal los phreakers son personas con conocimientos insuperables sobre los sistemas telefónicos, incluso más que los propios técnicos de las compañías telefónicas. Asimismo, poseen profundos conocimientos de tarjetas prepago y amplios conocimientos sobre informática. Dentro de las actuales manifestaciones de phreaking este autor distingue las siguientes modalidades:

1. Shoulder-surfing: conducta que realiza el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, obteniéndolo al momento en que la víctima lo utiliza y sin que pueda percatarse de que está siendo observada por este sujeto, quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.
2. Call-sell operations: en este caso, la acción del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta es una técnica que ha sido aprovechada a nivel internacional por los traficantes de drogas.
3. Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección.
4. Acceso o no autorizado a sistemas de correos de voz: el sujeto activo ataca las máquinas destinadas al almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio, pudiendo perseguir

⁷⁵ Orts Berenguer, E. y Roig Torres, M. Delitos informáticos y delitos comunes..., op. cit., p. 181.

por esta vía diversos objetivos, como el utilizar los códigos de transferencia de mensajería automática manejados por el sistema o lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

5. Monitoreo pasivo: técnica a través de la cual el sujeto intercepta ondas radiales para acceder a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.⁷⁶



Vanguardia en
Ciencias Penales

Instituto de Formación Profesional

Biblioteca

⁷⁶ Morant Vidal, J. Protección penal de la intimidad..., op. cit., pp. 44-45.

CAPÍTULO V

Sujeto pasivo

Es la persona o entidad sobre la cual recae la conducta que realiza por el sujeto activo. La mayoría de los delitos informáticos no son descubiertos, pero es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica.

Por lo que hace al sujeto activo, Gutiérrez Francés señala que los sectores más afectados por la criminalidad mediante computadoras son la banca, la enseñanza, instituciones públicas, industria de transformación y de seguros fundamentalmente y que, además, en estos sectores, bien por imperativo legal, bien por las características del tráfico económico, operan casi exclusivamente personas jurídicas, la conclusión es fácil: la víctima por excelencia del ilícito informático es la persona jurídica. Pero, además, se trata de personas jurídicas con un potencial económico muy elevado y que, por lo general, no suelen gozar de muy buena prensa entre el ciudadano medio.⁷⁷

Por su parte, Rovira del Canto afirma que ha habido una inicial extensión de la conceptualización del potencial sujeto pasivo de estos delitos, pudiendo comprenderse con carácter general no sólo a los titulares y demás beneficiarios legítimos de un sistema informático, como los usuarios y terceros de buena fe, sino incluso a cualquier persona, física o jurídica, que en cualquier momento, ocasión, o circunstancia tenga o se encuentre

⁷⁷ Gutiérrez Francés, M. de la L. Fraude informático y estafa, Ministerio de justicia, Madrid, 1991, p. 76.

vinculado directa o indirectamente con un sistema informático, la información en él contenida, o los datos que la representan.⁷⁸

Desde mi punto de vista, tenemos que distinguir qué sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo y, en el caso de los delitos informáticos, las víctimas pueden ser individuos, instituciones, empresas, gobiernos, etc., que usan sistemas automatizados de información, redes informáticas, etc.

El sujeto pasivo de los delitos que nos ocupan es sumamente importante ya que, mediante él, podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos debido a que, muchos de éstos, son descubiertos casualmente por el desconocimiento del modus operandi de los sujetos activos.

Por lo anterior, ha sido imposible conocer la verdadera magnitud de los delitos informáticos ya que, como se mencionó anteriormente, la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables. Si a esto se le suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionarles, aunado a las pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan bajo la sombra de la cifra negra u oculta.

Por todo esto, se reconoce que para conseguir una previsión efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que, educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para destacar, investigar y prevenir los delitos informáticos.

⁷⁸ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 115.

CAPÍTULO VI

Las amenazas de internet a la información

Las amenazas en Internet están latentes para todos los usuarios que ingresan al mismo.

La palabra "amenaza" proviene del latín minaciense,⁷⁹ y significa dar a entender con actos o palabras que se le quiere hacer un mal a otro.⁸⁰ En el lenguaje informático se denomina "amenaza" a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) que podría efectuar una persona, máquina, suceso o idea, dada una oportunidad. Un ataque es la realización de una amenaza.⁸¹

Existen cuatro categorías generales de amenazas o ataques, a saber:

- a. *Interrupción*: Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente.⁸²

⁷⁹ (a- I + lat. minacia, amenaza) tr.-intr. Dar a entender [a uno] la intención de hacerle algún mal: ~ a alguien al pecho; ~ con la espada; ~ de muerte. 2 Dar indicios de estar inminente [una cosa mala o desagradable]: el edificio amenaza ruina. CONJUG. como realizar. Enciclopedia Microsoft Encarta 2002. 1993-2001 Microsoft Corporation.

⁸⁰ Diccionario Jurídico Mexicano, Primer Tomo, 14 ed., Editorial Porrúa, México 2000, p. 149.

⁸¹ <http://www.delitosinformaticos.com/articulos/freenet.htm>. Consultada el 15 de Enero del 2006.

⁸² Ejemplo: destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.

- b. *Intercepción*: El ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o un ordenador.⁸³
- c. *Modificación*: Un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo.⁸⁴
- d. *Fabricación*: Un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema.⁸⁵

Los ataques en Internet pueden ser pasivos o activos. En los pasivos, el atacante no altera la comunicación, sino que únicamente la observa, con el fin de obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Unas técnicas más sutiles para obtener información de la comunicación pueden consistir en:

- a. Obtención del origen y destinatario de la comunicación, leyendo los asuntos de los mensajes interceptados.
- b. Control del volumen de tráfico intercambiado entre las entidades interceptadas, obteniendo así información acerca de la actividad o la inactividad inusuales.
- c. Control de las horas habituales de intercambio de datos entre las entidades de comunicación, para extraer información acerca de los periodos de actividad.

Al igual que los sujetos en la Red, los ataques, tanto activos como pasivos, no pueden ser enumerados de forma limitada, ya que diariamente surgen nuevas formas.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, sin embargo, es posible evitar su éxito mediante el cifrado de la información.

⁸³ Ejemplos de este tipo de ataques son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulan por la Red, o bien la lectura de las cabeceras de mensajes para descubrir la identidad de uno o más de los usuarios involucrados en una comunicación que es interceptada ilegalmente.

⁸⁴ Ejemplo: el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la Red.

⁸⁵ Ejemplos de este ataque son: insertar mensajes no deseados en una red o añadir registros a un archivo.

Los ataques activos implican algún tipo de modificación en el proceso de transmisión de información a través de la Red o la creación de un falso proceso de transmisión, pudiendo subdividirse en cuatro categorías:

- a. *Suplantación de identidad*: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.⁸⁶
- b. *Reactuación*: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.⁸⁷
- c. *Modificación de mensajes*: una parte del mensaje legítimo es alterada o los mensajes son retardados o reordenados para producir un efecto no autorizado.⁸⁸
- d. *Degradación fraudulenta del servicio*: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones.⁸⁹

Dado lo expuesto, resulta que la información que viaja por Internet puede ser fácilmente interceptada y utilizada para fines diversos a los propuestos por su dueño, por esto es imperativo regular la forma en que viaja esa información, castigando a los "individuos" que se hacen de la misma en forma "ilícita".

⁸⁶ Ejemplo: secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

⁸⁷ Ejemplo: ingresar dinero varias veces en una cuenta dada.

⁸⁸ Ejemplo: el mensaje "ingresa diez mil dólares en la cuenta A" podría ser modificado para decir "ingresa diez mil dólares en la cuenta B".

⁸⁹ El intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red, inundándola con mensajes no deseados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, web, FTP, etc.

CAPÍTULO VII

La criminalidad informática

Es cierto que debido al gran avance que han sufrido las comunicaciones en las últimas décadas, actualmente se logran cosas que anteriormente eran objeto de películas de ciencia ficción. Sin embargo, las formas de criminalidad han evolucionado junto a ese gran avance atentando incluso contra el mismo.

Internet se ha hecho de suma importancia para personas que tratan de aprovecharse de los demás usuarios, utilizándolo para cometer "delitos tradicionales" de formas no tradicionales.⁹⁰

La enorme evolución de la informática ha transformado al mundo en una gran tecnología que nos facilita el trabajo diario, aunque así como ha transformado al mundo, la tecnología también ha transformado las antiguas conductas delictivas en los ahora llamados "delitos informáticos".

La piratería informática⁹¹ provoca pérdidas de 3,705 millones

⁹⁰ Ejemplo: fraudes en internet.

⁹¹ Un comité clave del Parlamento Europeo aprobó el proyecto final de una norma europea para combatir la piratería en Internet. La votación del comité de asuntos legales del Parlamento Europeo, órgano legislativo de la Unión Europea, había sido esperada ansiosamente por las industrias de la música y el cine, que cada año pierden millones a causa de la piratería digital. "El texto ha sido aprobado. Hemos defendido una posición que está con el interés de los autores", dijo a Reuters Enrico Boselli, miembro del comité parlamentario. La mencionada norma dará a los propietarios de la música y las obras de cine el derecho a utilizar tecnología avanzada, como codificación especial, para bloquear las copias ilícitas de trabajos

de dólares en Europa. La progresiva implantación de las nuevas tecnologías en todos los ámbitos de la denominada sociedad de la información ha disparado el uso ilegal de aplicaciones de software en todo el mundo. En 1999 se hicieron famosos los virus⁹² Melissa,⁹³

registrados y limitar la captura ilegal de archivos de audio y video desde Internet. La redacción del proyecto final resultó una gran tarea para la comisión del Parlamento Europeo, a causa del choque de intereses de grupos de presión. Mientras los autores y las compañías de música querían la inclusión de reglas muy duras contra las copias ilegales, las asociaciones de consumidores se quejaron de que tales disposiciones podrían limitar las libertades individuales. <http://www.deltosinformaticos.com-/articulos/freenet.htm>. Consultada el 26 de enero de 2005.

⁹² El primer virus del mundo fue creado en 1982, denominado "Elk Cloner" y su autoría corresponde a Rich Skrenta, quien en ese entonces era un muchacho de sólo 14 años de edad. El virus fue escrito para las máquinas Apple II, que al infectarse mostraban el siguiente mensaje en pantalla por cada cincuenta veces que se encendiese la ordenador: Elk Cloner: The program with a personality. It will get on all your disks. It will infiltrate your chips, Yes it's Cloner! It will stick to you like glue, it will modify RAM too, send in the Cloner! Al tratarse de un período en que Internet era un sistema limitado a los círculos académicos, la propagación de Elk Cloner se producía mediante disquetes. El primer virus que llamó la atención mediática a nivel mundial fue "Jerusalén", que luego de propagarse silenciosamente liberaba su carga destructiva cada viernes 13, eliminando archivos en las máquinas infectadas. <http://www.diarioti.com/noticias/2000/may2000/15193090.htm>. Consultada el 26 de enero del año 2005. El último virus aparecido hasta el 05 de Marzo del año 2001 es el virus conocido como ROJ_MYBABYPIC.A. El mismo consigue distribuirse automáticamente por Internet a través de archivos ejecutables adjuntos a mensajes de correo electrónico con el asunto "My Babypic". Adicionalmente incluye rutinas maliciosas que pueden dañar información de los sistemas afectados. Este virus se propaga por e-mail (MS Outlook) llegando al usuario como un archivo adjunto a un mensaje con asunto "My Babypic". Cuando el archivo .EXE es ejecutado, una ventana con la foto de un niño es desplegada. Una vez que la ventana se cierra, el troyano crea varias copias de sí mismo en la carpeta Windows/System con los siguientes nombres de archivos: El asunto del mensaje del virus es "My Babypic"; el cuerpo del mensaje dice: "It's my animated baby picture!!!" y además llega un archivo adjunto bajo el nombre "MYBABYPIC.EXE". En sistemas Windows NT, el archivo CMD.EXE citado anteriormente sobrescribe el archivo original del sistema operativo. El troyano cambia las entradas en el registro para lograr ser ejecutado cada vez que se reinicia el sistema. Una vez ejecutado intenta acceder a un sitio web específico (<http://www.youvebeenhacked.com>) y activar algunas rutinas maliciosas que van desde sobrescribir archivos con ciertas extensiones hasta borrarlos. En particular el troyano sobrescribe con su propio código los archivos con las siguientes extensiones: C, CPP, CSS, H, HTA, JPG, JPEG, JS, JSE, PAS, PBL, SCT, y WSH, agregando la extensión .EXE. Su rutina de borrado se ejecuta con archivos del tipo .VBS y .VBE. Adicionalmente crea copias de sí mismo usando los nombres de los archivos .MP2, .MP3 y .M3U existentes. Los archivos originales permanecen ocultos y las copias infectadas quedan como archivos ejecutables. El virus abruptamente puede habilitar y deshabilitar las teclas Numlock, ScrollLock y CapsLock.

⁹³ Hasta el surgimiento del I LOVE YOU, el virus más costoso de la historia había

Chernovyl, Explore Zip, Babylonía y Bubbleboy; en el año 2000 el virus I LOVE YOU causó daños, en algunos casos irreparables.⁹⁴ Los fraudes en Internet aumentaron significativamente en el mismo año y representaron dos tercios del total de casos presentados en el Servicio de Crímenes Comerciales de la Cámara de Comercio Internacional (ICC). Según el informe, 2,776 de los 4,139 casos referidos por sus miembros estuvieron directamente relacionados con el crimen, fraude y falsificación a través de sitios web que ofrecen mercancía o servicios falsos; dicha encuesta mostró que en el año 2000 esta oficina salvó a sus miembros de pérdidas de alrededor de 2 millones 300 mil dólares, advirtiéndoles acerca de las negociaciones con esta nueva generación de criminales que habían sido previamente investigados".⁹⁵

Por "criminalidad informática" se pueden señalar conductas como la burla a los sistemas de dispositivos de seguridad, tanto en cajeros automáticos, como en máquinas tragamonedas, manipulaciones técnicas en el sistema de televisión pagada, invasiones a computadoras, correos o sistemas mediante una clave de acceso, revelación de secretos por parte del personal de la institución bancaria, fraudes en la telefonía celular móvil, conductas antisociales de personas que ingresan a sistemas no autorizados, sustracción de información, envío de mensajes falsos, hasta la alteración de datos que provocan cada vez más pérdidas de miles de millones de dólares cada año.

Baón Ramírez define a la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.⁹⁶

Tiedemann comenta que la expresión "criminalidad mediante computadoras" alude a todos los actos antijurídicos, según la ley penal vigente, realizados con el empleo de un equipo automático de procesa-

sido Melissa, creado por el estadounidense David Smith, y que ocasionó pérdidas mundiales del orden de los 80 millones de dólares. Tal cifra es modesta comparada con los 15 mil millones de dólares en que se calculan los daños causados por ILOVEYOU, cuya presunta autoría se atribuye al filipino Onel Guzmán.

⁹⁴ Muñoz Machado, Santiago. La regulación de la Red. Poder y derecho en Internet. Grupo Santillana de Ediciones, 1998, p. 152.

⁹⁵ www.rpp.com.pe. Consultada el 21 de enero del 2005.

⁹⁶ <http://www.publicaciones.derecho.org/redi/No.06.Enero.de.1999/cuervo>. Consultada el 26 de enero de 2005.

miento de datos.⁹⁷ La utilización de computadoras en la economía, industria y, sobre todo, en el sector de bancos y seguros, genera también la aparición de nuevas formas de conductas delictivas que pronostican,⁹⁸ desde ya, el origen de una criminalidad informática transnacional.⁹⁹ En consecuencia, la interconexión global posibilitada por el Internet trae consigo una nueva calidad de criminalidad que afecta numerosos ámbitos de la vida y la economía. Ahora bien, el concepto de "criminalidad informática transnacional" no se deberá de confundir con el término "criminalidad organizada", ya que la criminalidad informática será transnacional cuando las conductas delictuales traspasen las fronteras de los países.

⁹⁷ Igualmente en http://www.publicaciones.derecho.org/redi/No.06_Enero_de_1999/cuervo. Consultada el 28 de enero año 2005.

⁹⁸ Tiedemann, Klaus. Derecho penal y nuevas formas de criminalidad, Lima, Idemsa, 2000. p. 85. "Ya que, hasta el momento no se ha demostrado tal internacionalización del fraude informático -aparte del abuso turístico de cajeros automáticos de bancos y del empleo que hagan bandas criminales de las tarjetas (de crédito) robadas en el extranjero- y también la interconexión internacional de los sistemas que, sin duda, será más fuerte en el futuro y es mencionada".

⁹⁹ En este sentido, Tiedemann, Klaus. Derecho Penal..., op. cit., p. 85 y ss. En donde explica la relación entre la criminalidad informática y el derecho penal. Así, el autor pronostica que debido al creciente empleo de sistemas procesadores de datos... en el futuro... la cuota de autores externos (debería) incrementarse; como consecuencia de la constitución de formas delictivas técnicamente cada vez más refinadas, al mismo tiempo sería probable un desplazamiento de círculo de víctimas, así como la aparición de una criminalidad informática transnacional.

CAPÍTULO VIII

Nociones generales del delito

Antes de entrar en el análisis de los delitos informáticos hay que entender lo que es un delito. Etimológicamente la palabra delito procede del latín "delictum", que significa abandonar el camino prescrito por la ley. Sociológicamente se entiende como una conducta desplegada por un ser humano, calificada como nociva para la sociedad en la que convive. Dicha calificación es realizada de acuerdo con el momento histórico; de aquí que existan conductas que sean consideradas como delitos en determinadas circunstancias de modo, tiempo y lugar, y al variar las mismas dicha conducta deja de considerarse como delito. Cabe destacar que la conducta castigada (llámese delito), presupone la existencia de bienes jurídicamente tutelados, mismos que pueden ser, por citar algunos, la "vida o formación del estado", la vida de una persona, la libertad, la salud, la integridad, el patrimonio, etc; en algunas ocasiones se ha llegado a extremos increíbles, como lo fue durante la Segunda Guerra Mundial, cuando en Alemania se creó un delito sobre todo aquello que dañara o pudiera dañar al Reich.¹⁰⁰

¹⁰⁰ Tema relacionado con el "sano sentimiento del pueblo", dentro de la quinta etapa del tipo penal, propuesta por la escuela de Kiel; ver Orellano Wiarco, O. Teoría del delito. Sistemas Causalista y Finalista, Editorial Porrúa, México, 1995, p. 20.

públicas, daños, delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores, sustracción de cosa propia a su utilidad social o cultural, delitos societarios y receptación, así como otras figuras afines.

Asimismo, el Código Penal no hace la distinción de qué figuras delictivas se comprenden dentro de los delitos contra el patrimonio y cuáles en los delitos contra el orden socioeconómico, por lo que se podría concluir que dentro de los delitos contra el patrimonio se comprenden las siguientes figuras: hurtos, robos, extorsión, robo y hurto de uso de vehículos, usurpación, defraudaciones y daños, y dentro de los delitos socioeconómicos estarían las insolvencias punibles, alteraciones de precios en concursos y subastas públicas, delitos relativos a la propiedad intelectual e industrial, delitos relativos al mercado y a los consumidores, sustracción de cosa propia a su utilidad social o cultural, delitos societarios y receptación, así como otras figuras afines.

Antes de seguir hablando de los delitos contra el patrimonio, considero necesario señalar qué es lo que se entiende por patrimonio, es importante mencionar que existen distintas teorías en cuanto al concepto de patrimonio se refiere, así existen tres concepciones distintas que tratan de definir el término de patrimonio, de esta manera tenemos:

- 1.- Concepción jurídica del patrimonio.
- 2.- Concepción económica del patrimonio.
- 3.- Concepción mixta del patrimonio.

La "concepción jurídica del patrimonio" establece que el patrimonio comprende los derechos subjetivos patrimoniales de la persona, ya sean reconocidos por el derecho público, ya por el privado, y establece que los derechos o las cosas que se detentan sin contar con la protección del derecho pueden ser considerados elementos del mismo.

La "concepción económica del patrimonio" establece que éste se concibe como el conjunto de bienes que se encuentran bajo el poder fáctico de una persona, con independencia de que su relación con ellos se concrete o no en un derecho o de que sea o no susceptible de reconocimiento jurídico.

Por último la "concepción mixta del patrimonio", que es la dominante en nuestra doctrina. En términos de esta concepción, para Antón Oneca, el patrimonio puede definirse como "el conjunto de valores económicos jurídicamente reconocidos, comprendiendo cosas muebles

e inmuebles, propiedad, posesión, derechos de crédito, derechos de uso y demás derechos reales y personales, valorables en dinero, con tal de que tengan reconocimiento por parte del derecho, siquiera sea provisional".¹⁰²

González Rus, por su parte, manifiesta que esta definición es la que mejor se corresponde con el Código, en el que se protegen los elementos integrantes del patrimonio y explica que así se considera siempre sujeto pasivo del delito al titular del derecho sobre la cosa, y por qué todas las figuras delictivas del título presuponen que la cosa objeto del delito tiene valor económico, siendo éste el que se toma como referencia, en su caso, para la diferenciación entre el delito y la falta.¹⁰³

Para Muñoz Conde el patrimonio es "el conjunto de derechos y obligaciones, referibles a cosas u otras entidades, que tienen un valor económico y que deben ser valorables en dinero", asimismo señala que lo que caracteriza al concepto penal de patrimonio es tanto el valor económico de la cosa, como la protección jurídica que se brinda a la relación de una persona con esa cosa. Por ello, cree conveniente aceptar la concepción mixta jurídica y económica de patrimonio, mencionando además que esta concepción mixta se caracteriza por los siguientes puntos:

Objeto material de un delito patrimonial sólo pueden serlo aquellos bienes dotados de valor económico.

Para ser sujeto pasivo de un delito patrimonial no basta con que el sujeto tenga una relación meramente fáctica con la cosa, sino que es preciso que esté relacionado con ella en virtud una relación protegida por el ordenamiento jurídico.

[...] Por perjuicio patrimonial hay que entender toda disminución, económicamente evaluable que el acervo patrimonial cree, jurídicamente, corresponde a una persona.¹⁰⁴

Desde mi punto de vista, la concepción mixta del patrimonio es la más adecuada, ya que se entiende de esta manera que el patrimonio siempre tendrá o deberá de tener un valor económico estimable

¹⁰² Cita en González Rus, J. J. "Delitos contra el patrimonio y contra el orden socioeconómico (I)", en Compendio de derecho penal español. Parte Especial, Cobo del Rosal, M. (dir.) Editorial Marcial Pons, Madrid, 2000, p. 377.

¹⁰³ Ibidem.

¹⁰⁴ Muñoz Conde, F. Derecho Penal. Parte Especial, Editorial Tirant lo Blanch, Valencia, 2002, pp. 352-353.

en dinero, y así se puede entender el patrimonio como un conjunto de derechos y obligaciones (que involucran tanto lo jurídico, como lo patrimonial), que son siempre valorables en dinero.

Por otro lado el ya mencionado Título XIII del Libro II del Código Penal, también hace mención de los Delitos contra el Orden Socioeconómico. Desde este punto de vista tenemos que, para Vives Antón y González Cussac el Derecho Penal Económico se refiere al conjunto de normas jurídico penales que protegen el orden "socioeconómico", entendiendo éste en sentido estricto, como participación estatal en la economía, o en sentido amplio como el conjunto de normas protectoras de la producción, distribución y consumo de bienes y servicios.¹⁰⁵

Por último, en mi opinión se puede entender que los delitos socioeconómicos suponen la lesión de bienes jurídicos relacionados con la regulación jurídica de la producción, distribución y consumo de bienes y servicios, mientras que los delitos contra el patrimonio son aquellos que atacan el patrimonio (bien jurídicamente protegido), que causan un perjuicio, es decir, una disminución o una afectación en los bienes o derechos (patrimonio) de una persona y que pueden ser valorados en dinero y protegen estos bienes desde una perspectiva particular o privada.

¹⁰⁵ Vives Antón, T.S., González Cussac, J.L., Derecho penal. Parte Especial, Editorial Tirant lo Blanch, Valencia, 1999, p. 352.

CAPÍTULO X Clasificaciones

Entre las clasificaciones de los delitos patrimoniales y de los delitos socioeconómicos existen varios autores que intentan aclarar cuáles son los patrimoniales y cuáles son los económicos, así tenemos que, según Alonso Pérez, los delitos patrimoniales se pueden clasificar atendiendo a diversos criterios, de esta manera, según el medio utilizado, distingue:

- a) Delitos patrimoniales con violencia o intimidación en las personas (robo con violencia o intimidación, extorsión, etc.).
- b) Delitos patrimoniales con fuerza en las cosas (robo o con fuerza).
- c) Delitos patrimoniales sin violencia o intimidación en las personas ni fuerza en las cosas (hurto, apropiación indebida, etc.).
- d) Delitos patrimoniales con engaño (estafa).

Según el objeto sobre el que recaen:

- a) Delitos patrimoniales sobre inmuebles (usurpación, estafas inmobiliarias, etc.).
- b) Delitos patrimoniales sobre muebles (hurto, robo, etc.).

Según exista o no enriquecimiento del autor:

- a) Delitos patrimoniales de enriquecimiento, mediante apoderamiento (hurto, robo y usurpación), defraudación (estafa, apro-

piación indebida) o explotación o negocio (maquinaciones para alterar el precio de las cosas, usura, recetas, etc.).

- b) Delitos patrimoniales sin enriquecimiento (hurto de cosa propia, daños, incendios, etc.).¹⁰⁶

Por otro lado, Calderón Cerezo distingue los delitos patrimoniales de los socioeconómicos, así tenemos:

- a) Delitos patrimoniales.

Entre los delitos patrimoniales que no comportan enriquecimiento únicamente se incluyen los daños.

- b) Con enriquecimiento:

De apoderamiento material: hurto, robo, robo y hurto de uso de vehículos de motor; de apoderamiento jurídico de derechos reales o bienes inmuebles ajenos, usurpación y extorsión.

Defraudación en función de que el engaño constituya, en todo o en parte, el medio comisivo: estafa, apropiación indebida, defraudación de fluido eléctrico y análogos e insolvencias punibles. Entre los delitos económicos se incluyen los siguientes: alteración de los precios en concursos y subastas públicas; relativos a la propiedad intelectual e industrial; relativos al mercado y a los consumidores; sustracción de cosa propia a su utilidad social; delitos societarios, y receptación y otras conductas afines entre las que destacan las de "blanqueo de capitales".¹⁰⁷

Por otro lado, para Muñoz Conde los delitos contenidos en el título XIII, del Libro II del Código Penal, se pueden clasificar en: delitos contra el patrimonio y delitos contra el orden socioeconómico; pero a su vez los delitos contra el patrimonio los clasifica en:

- I. Delitos patrimoniales de enriquecimiento.

- A) *De apoderamiento:* bien tomando materialmente una cosa mueble (robo, hurto, acuso de vehículos de motor), bien usurpando un derecho real o cosa inmueble (usurpación).
B) *Defraudaciones:* bien desempeñando el fraude o engaño el pa-

¹⁰⁶ Alonso Pérez, F. Delitos contra el patrimonio y contra el orden socioeconómico. Aspectos penales y criminológicos, Editorial Colex, Madrid, 2003, pp. 29-30.

¹⁰⁷ Calderón Cerezo, A., Choclán Montalvo, J.A., Derecho penal. Parte Especial, Tomo II, Editorial Bosch, Barcelona, 2001, p. 222.

pel rector (estafa, apropiación indebida, defraudaciones del fluido eléctrico y similares), bien teniendo un papel meramente accesorio o concomitante (insolvencias punibles).

- II. Delitos patrimoniales sin enriquecimiento: daños.¹⁰⁸

Una vez que hemos tratado de diferenciar lo que son o, mejor dicho, lo que comprenden, los delitos patrimoniales y los delitos socioeconómicos, y habiéndolos analizado y clasificado, entraremos al tema de los delitos informáticos en el ámbito económico.

Así tenemos que, en cuanto al tema de la criminalidad económica vinculada con la informática, Choclán Montalvo distingue:

- a) De un lado, los atentados patrimoniales contra elementos informáticos que abarcan aquellas manifestaciones delictivas que tienen como objeto material un elemento informático, bien físico o hardware (teclado, monitor, CPU, disquetes, etc.), bien lógico o software (datos, información, programas, etc.). En este grupo cabe situar los ilícitos consistentes en hurto, robo, apropiación indebida del ordenador, sabotaje y espionaje informático, descubrimiento, revelación de secretos, competencia ilícita, hurto de datos, etcétera.
b) De otro lado, los atentados patrimoniales realizados por medio del sistema informático, en cuyo grupo se ubican las defraudaciones cometidas a través del sistema informático, fundamentalmente por la introducción de datos falsos o manipulaciones del programa.¹⁰⁹

Asimismo, manifiesta que lo característico de la criminalidad informática patrimonial es la lesión de un patrimonio que tiene lugar por una intervención del sujeto activo en un sistema informático, o bien por el ataque a la propiedad de los datos procesados, sin que las agresiones al hardware constituyan, por lo general, acciones punibles que puedan considerarse específicas respecto de los ilícitos patrimoniales en general.

Por otro lado, clasifica los delitos económicos vinculados a la informática, de la siguiente manera:

- a) Fraude mediante manipulaciones contra los sistemas de procesamiento de datos;

¹⁰⁸ Muñoz Conde, F. Derecho penal. Parte Especial..., op. cit., pp. 352-353.
¹⁰⁹ Choclán Montalvo, J.A. Fraude informático..., op. cit., pp. 315-319.

- b) El sabotaje informático o daño contra los elementos lógicos del sistema informático;
- c) El espionaje industrial hoy descubrimiento de los secretos de empresa;
- d) El hurto de software o hurto informático.¹¹⁰

Por su parte, Sieber clasifica los delitos económicos vinculados a la informática, distinguiendo:

- 1. Fraude mediante manipulaciones contra los sistemas de procesamiento de datos;
- 2. Espionaje informático y robo (hurto) de software;
- 3. Sabotaje informático;
- 4. Apropiación de servicios;
- 5. Acceso no autorizado a los sistemas informáticos;
- 6. Fraude fiscal informático.¹¹¹

Desde el punto de vista del Derecho penal económico, una clasificación bastante aceptada por la doctrina moderna distingue la criminalidad informática en cuatro grupos:

- 1º Espionaje informático, como invasiones no autorizadas en instalaciones (y programas) ajenos e investigaciones de datos ajenos, dentro del cual incluye el hacking.
- 2º Sabotaje informático, o deterioro o destrucción de datos.
- 3º Manipulación informática, esto es la alteración de datos con el objetivo de influir en el resultado del procesamiento de datos.
- 4º Hurto del tiempo: utilización no autorizada del tiempo de procesamiento de un ordenador.

Rovira del Canto, dentro de los ilícitos informáticos en el ámbito económico, distingue las siguientes modalidades básicas:

- 1. Acceso informático ilegal o hacking informático.
- 2. Hurto de tiempo informático.

¹¹⁰ Ídem.

¹¹¹ Gutiérrez Frances, M. de la L. Fraude informático y estafa..., op. cit., p. 60.

- 3. Espionaje informático.
- 4. Piratería de software y piratería de otros tipos de productos.
- 5. Sabotaje informático.
- 6. Fraude informático.¹¹²

Como podemos ver, casi todas las clasificaciones antes mencionadas, prácticamente contemplan las mismas modalidades delictivas por lo que, a continuación, trataremos de explicar en que consisten cada una de ellas.

¹¹² Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 192.

CAPÍTULO XI Modalidades

11.1 Intrusismo informático o hacking informático

Una vez que ha quedado definido el término hacking, en el apartado dedicado al estudio y análisis de las características del sujeto activo en los delitos informáticos y, en concreto, de las conductas de hacking, a manera de conclusión podemos entender que este término se usa tradicionalmente para describir la mera entrada o acceso a sistemas informáticos por el simple gusto de superar las medidas de seguridad de los sistemas informáticos, sin intención o sin la finalidad de manipular, defraudar, cometer sabotaje o espionaje informático.

El acceso puede darse de forma directa. El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrir las deficiencias a las medidas existentes de seguridad. A menudo los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia con que los usuarios utilizan contraseñas comunes.

El intrusismo informático, para gran parte de la doctrina que está en pro de la no previsión penal de las conductas de hacking, considera que en este tipo de conductas no existe un ánimo de lucro en el sujeto que realiza la conducta, así como tampoco existe un perjuicio patrimonial efectivo en el sujeto pasivo de la conducta delictiva, quien normalmente es el titular del sistema, equipo, o red que fue objeto del acceso ilegal y por lo tanto no queda claro, o no ésta bien

establecido, cuál es el bien patrimonial o económico que jurídicamente se debe de proteger.

En este sentido, Morón Lerma señala que la primera duda que surge en las conductas de intrusismo informático es la ubicación sistemática de este delito de peligro de la seguridad de los sistemas informáticos, y añade que no parece conveniente forzar su encaje en un título dedicado a los delitos contra el patrimonio y contra el orden socioeconómico, cuando la seguridad vulnerada sea la de una universidad, que ve perturbado el funcionamiento de sus servicios bibliotecarios a distancia o telemáticos, como consecuencia de conductas de hacking.¹¹³

Desde este punto de vista, estas conductas no son ni serían catalogadas como delitos informáticos de carácter económico o patrimonial, cosa que desde mi punto de vista se debería de diferenciar, en el sentido de que si de la mera conducta de intrusismo informático no se derivan otras conductas más graves en el ámbito de la informática, estaríamos hablando de un delito contra la intimidad. Si, por el contrario, efectivamente se derivan otras conductas más graves, sí estaríamos hablando de un delito de carácter patrimonial o económico, ya que si bien es cierto que el sujeto activo en un principio no posee un ánimo de lucro con tal conducta, sí obtiene con estas conductas determinados conocimientos técnicos sobre las barreras de seguridad informáticas, y obtiene mayor capacidad, experiencia y conocimientos que le hará más fácil acceder a diferentes equipos, sistemas y redes informáticas, sin autorización de los titulares de éstos, ocasionando en este supuesto conductas más graves, como sería el de obtener secretos de personas, de empresas o causar un daño.

Asimismo, y por lo que hace al perjuicio patrimonial que pueda sufrir el sujeto pasivo, es preciso manifestar que si bien es cierto, en la mayoría de los casos, la o las personas afectadas por este tipo de conductas no resultan perjudicadas patrimonialmente, sí se ponen en riesgo sus intereses económicos contenidos en los programas o en los datos que tratan de protegerse y porque, precisamente, los titulares de los sistemas, redes o equipos, han establecido una serie de medidas de seguridad para evitar que personas ajenas a determinada información tengan acceso a ésta. Con lo que, desde mi punto de vista, sí existiría un perjuicio para las personas o titulares de los sistemas informáticos,

¹¹³ Moron Lerma, E. Internet y Derecho Penal..., op. cit., p. 79.

aunque es de reconocerse que es extremadamente difícil calcular patrimonialmente el daño o perjuicio que se causa con la conducta de mero intrusismo informático. Distinto es, como ya se mencionó, que los accesos no autorizados concluyan en conductas o resultados más graves, ya sea que el sujeto activo realice la intrusión como un medio necesario para conseguir, por ejemplo, intimidades ajenas, secretos de empresa, destruir datos, etc., en cuyo caso, el mero acceso quedaría absorbido por la conducta o el resultado final, siendo de esta forma más fácil el determinar patrimonialmente el daño o perjuicio causado, considerando en estos supuestos un delito de carácter patrimonial o económico.

Por lo que, a manera de conclusión, considero que la mera conducta de intrusismo informático debe de ser considerada como un delito contra la intimidad y no como un delito de carácter patrimonial o económico y, por el contrario, debe de considerarse como un delito de estos tipos cuando derive en otras conductas más graves en el ámbito de la informática, que sí puedan cuantificarse en dinero.

Encuentro muy lógica y concuerdo ampliamente con lo manifestado por González Rus en el sentido de que el hacking es punible en lo relacionado con los diferentes tipos penales (piratería informática, daños informáticos, sabotaje informático, etc.), o en su caso por la vía de la tentativa de tales delitos si no se consuman éstos.¹¹⁴

En otras palabras, González Rus mantiene que "el curioso que se introduce en un sistema informático ajeno y husmea por el disco duro, aunque no sea más que para ver qué ficheros hay, lo hace para enterarse de qué cosas tiene el sujeto pasivo". Por tanto, le presupone este ánimo y por esa vía le imputa la comisión de los delitos, aun cuando esta comisión lo fuera en grado de tentativa.

Rovira del Canto, por su parte, manifiesta que sí existe un ánimo del lucro, que la doctrina y la jurisprudencia ha considerado y calificado como "ánimo de lucro jurídico", consistente en la obtención de ventajas personales, obteniendo además un prestigio o reconocimiento dentro de las cerradas comunidades y colectividades sociales interesadas por las nuevas tecnologías, sus deficiencias y su vulnerabilidad. Señala además que en cuanto al perjuicio efectivo, sí existe una clara puesta en peligro de los intereses económicos-patrimoniales, consistentes en el esfuerzo o costes en medidas de seguridad, que los titulares de los sistemas y redes informáticas han establecido para evitar accesos

¹¹⁴ De Alfonso Laso, D. El hackerin blanco..., op. cit., p. 522.

no autorizados, y menciona que al menos en estos casos, debe apreciarse que sí se viola o la formal "esfera de la privacidad y del secreto" o "la integridad del sistema informático afectado".¹¹⁵

Sieber manifiesta que las conductas de intrusismo informático que derivan en acciones más graves, desde el punto de vista de la informática, cuando llegan a conocerse, estos actos de piratería (hacking) pueden ser útiles para la detección de escapes en el sistema informático. De todos modos, generalmente son peligrosos, puesto que pueden destruirse datos por negligencia, pueden causarse bloqueos de sistemas, y la localización de deficiencias en la seguridad por acciones cometidas como retos que pueden permitir, a continuación, realizar fraudes financieros.¹¹⁶

Por su parte, Morón Lerma señala que las conductas de hacking son definidas por la doctrina especializada como meros accesos a sistemas informáticos perpetrados con un único fin, a saber, la vulneración de un password o puerta lógica. No hay duda de que, en ocasiones, estas conductas no se limitarán al mero acceso y devendrán antesala de otros ilícitos más graves. De la misma forma señala que los estudios criminológicos realizados en otros países demuestran comportamientos inicialmente de mero intrusismo informático, desprovistos de toda intención distinta al propio acceso no autorizado, y terminan convirtiéndose en otros ilícitos más graves como fraude, espionaje, sabotaje, etcétera. Una vez descubierta la puerta de entrada a un sistema, el hacker difícilmente se resiste a agotar las posibilidades que tiene a su alcance y comete atentados contra la intimidad, el patrimonio, etc.¹¹⁷

Rovira del Canto menciona que en muchos supuestos estas conductas de acceso ilegal aparecen configuradas materialmente como actos preparatorios de comportamientos delictivos informáticos más graves, en donde sí aparecen unos perjuicios considerables, que suceden cuando posteriormente los autores usan su experiencia y los conocimientos adquiridos con sus logros de acceso para cometer o favorecer la comisión por terceros de acciones o actos de espionaje, sabotaje o fraudes informáticos.¹¹⁸

¹¹⁵ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 196.

¹¹⁶ Sieber, Ulrich Criminalidad informática..., op. cit., pp. 77-78.

¹¹⁷ Moron Lerma, E. Internet y Derecho Penal..., op. cit., pp. 74-75.

¹¹⁸ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 196.

11.2 Hurto de tiempo informático

El hurto de tiempo informático consiste, en términos generales, en la utilización no autorizada del tiempo de procesamiento de un ordenador.

Existen diferentes modalidades, entre ellas encontramos:

- Robo de servicios o hurto de tiempo de ordenador. Cuando los empleados utilizan en una empresa horas de máquina sin autorización para realizar trabajos personales. Hoy en día este tipo de delito ha caído en desuso, debido a que en la actualidad es relativamente sencillo acceder a un ordenador, pero esto no era así hace unos años, cuando las grandes computadoras eran propiedad de las empresas debido al alto costo de las mismas.
- Apropiación de informaciones residuales, que han sido abandonadas por sus legítimos usuarios de servicios informáticos como residuo de determinadas operaciones.
- Parasitismo informático. Se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente. Suele asociarse a esta figura la de la suplantación de personal que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios informáticos.

Para Sieber el hurto de tiempo es aquél en el que los empleados del proceso de datos utilizan las computadoras de la empresa y parcialmente también sus programas, para fines privados y actividades complementarias.¹¹⁹ En estos casos sólo se produce un daño realmente importante para la empresa en el caso de abuso en el ámbito del teleproceso, así como en casos en los que la empresa tiene que pagar el tiempo utilizado por un ordenador de alquiler o en los que el autor atrae clientes de su empresario.

Para Davara Rodríguez consiste en la "utilización de un ordenador o programas ajenos, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro".¹²⁰

¹¹⁹ Sieber, Ulrich. Criminalidad informática..., op. cit., p. 27.

¹²⁰ Davara Rodríguez, M.A., Manual de derecho informático..., op. cit., p. 292.

Choclán Montalvo manifiesta que el hurto de tiempo consiste en la utilización de un sistema informático sin costo.¹²¹

Para Rovira del Canto consiste en "toda acción de utilización o uso subrepticio de un equipo, sistema o red informática o telemática ajena, con ánimo del lucro y en perjuicio de su titular".¹²²

De la misma manera, este autor distingue diversas modalidades:

- a.- El hurto de tiempo compartido (timesharing) permite aprovecharse del tiempo asignado a otro usuario en el procesamiento o transferencia de información o datos de un ordenador o equipo informático para utilizarlo conjuntamente en el procesamiento o transferencia de información propia.
- b.- El hurto de servicios informáticos, que permite aprovecharse a los empleados de instalaciones informáticas que utilizan los programas y el ordenador de su empresa para realizar trabajos de servicios a terceros con evidente lucro para ambos, y en perjuicio de la empresa titular de las computadoras y de los programas.
- c.- El hurto de tiempo informático, en stricto sensu, mediante el uso no autorizado de un ordenador o equipo informático o telemáticos para, aprovechándose del conjunto informático existente (hardware y software), utilizar en beneficio propio el tiempo de procesamiento y transmisión de información que permite tal equipo, con perjuicio del titular del mismo.

Asimismo, Moránt Vidal señala que el robo de servicios, especialmente el hurto de tiempo del ordenador, se refiere a supuestos de apropiación de informaciones residuales, y distingue dos modalidades:

- a) Scavenging, que implica la sustracción de datos que han sido abandonados por los legítimos usuarios de servicios informáticos como residuo de determinadas operaciones.
- b) Parasitismo informático (piggybacking), con el que se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos para utilizarlos en beneficio del delincuente.¹²³

¹²¹ Choclán Montalvo, J.A. Fraude informático..., op. cit., p. 352.

¹²² Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 205.

¹²³ Morant Vidal, J. Protección penal de la Intimidad..., op. cit., p. 47.

11.3 Espionaje informático

En la actualidad, los secretos empresariales y el valioso llamado know-how de las empresas y de las industrias se han convertido, en algunos casos, en los activos más valiosos de éstas, por lo que se les ha intentado proteger a toda costa, para así salvaguardar información extremadamente importante y valiosa. De esta forma, estos datos generalmente son almacenados mediante equipos informáticos. Como consecuencia han tomado relevancia las conductas cometidas por personas tendientes o encaminadas a conocer y adquirir los ilícitamente, y ha surgido así lo que se llama comúnmente espionaje informático.

El espionaje informático constituye una actividad especialmente peligrosa, ya que en los sistemas informáticos con frecuencia se almacenan gran cantidad de datos en espacios extremadamente pequeños siendo, en la mayoría de los casos, de suma importancia para personas, empresas, industrias y gobiernos.

Los objetos sobre los que recaen este tipo de acciones son principalmente programas informáticos, datos relevantes, ya sea de investigaciones, de seguridad o de defensa, datos relativos a la contabilidad o fabricación y distribución de empresas, bases de datos de clientes, etcétera, sin que, por lo general, resulten físicamente alterados ninguno de los elementos del hardware.

Para Sieber el espionaje informático y hurto de software constituye, en el ámbito de la criminalidad por ordenador, la segunda forma más frecuente del delito, y señala que para el sujeto activo esta actividad es especialmente lucrativa y para la empresa afectada especialmente peligrosa, ya que en los centros de cálculo de la mayoría de empresas con frecuencia se almacenan, en muy poco espacio, importantes y numerosos secretos de las mismas.¹²⁴

Asimismo, este autor señala que el objeto del espionaje informático está constituido, en todos los ámbitos, en primer lugar, por los respectivos programas y apunta que éstos aportan una fuente importante de conocimientos sobre la empresa; en el ámbito mercantil señala que son objeto de esta actividad los cálculos, los balances y las direcciones de clientes que se encuentran almacenados en el ordenador y, por lo que hace al ámbito técnico, el centro del interés se centra en los datos de desarrollo e investigación.

¹²⁴ Sieber, Ulrich. Criminalidad informática..., op. cit., pp. 22-25.

Por otro lado, Rovira del Canto define este tipo de actividades como "el conjunto de actividades de obtención no autorizada de datos o información de carácter sensible, esto es, confidenciales o secretos, de contenido y valor económico patrimonial, y/o divulgación no autorizada de los objetos legítimamente, con ánimo de lucro y en perjuicio de tercero".¹²⁵

Asimismo, Moránt Vidal señala que el espionaje informático, entre sus modalidades más notorias, destaca la fuga de datos, consistente en una versión informática de las tradicionales prácticas de espionaje industrial.¹²⁶

Por último, es importante señalar que para la mayoría de la doctrina el espionaje informático se encuentra limitado al ámbito estrictamente empresarial, comercial o industrial, ya que se le relaciona e identifica con el descubrimiento y revelación de secretos, siendo este planteamiento, desde mi punto de vista, erróneo ya que considero que pueden existir datos o información de carácter económico y patrimonial no relacionada a la empresa, industria o comercio.

11.4 Piratería informática

Por lo que hace al tema de la piratería informática, éste ya había sido analizado brevemente cuando se estudiaron las características del sujeto activo y, más concretamente, cuando se estudiaron las conductas de los llamados crackers. Ampliando el tema podemos afirmar que la piratería informática tradicionalmente se ha venido entendiendo como la copia y/o uso no autorizado de programas informáticos, también conocida como "hurto o robo de software".

En la actualidad, los programas o software se han convertido en una necesidad básica de toda empresa, industria o comercio, por lo que se venden en todas partes y a gran escala. Todo esto conlleva a que determinadas personas se dediquen a lucrar ilícitamente con la copia y distribución ilegal de estos programas. Asimismo, la piratería informática no puede quedar limitada a lo que se conoce como programas informático o software sino que, por el contrario, afecta en algunos casos en mayor medida a lo que se conoce como propiedad intelectual, esto es datos, películas, canciones, obras literarias etc. Así podemos ver que

¹²⁵ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 210.

¹²⁶ Morant Vidal, J. Protección penal de la intimidad..., op. cit., p. 47.

en cualquier esquina de algunos países es posible adquirir una copia ilegal ya sea de un programa de software, de una película en DVD, de un disco, etc.

Por otro lado, en la sociedad actual Internet se ha convertido, prácticamente, en un medio que se encuentra al alcance de la mayoría de las personas, lo que supone que es extremadamente fácil lograr, a través de Internet, una copia ilegal de programas, de datos, de películas, de canciones, etc., así como también distribuirlos de manera ilegal.

Más recientemente con la utilización del formato MP3, que comprime canciones, sonidos, películas, así como codifica datos y los reduce de forma considerable, haciendo posible su almacenaje en un gran número de aparatos de soporte informático de reciente creación, es cuando se ha agravado y agudizado el problema de la piratería informática, ya que se vuelve todavía más fácil, adquirir copias ilegales de datos, programas, canciones, películas, obras, etc.

Por último, para Rovira del Canto la piratería informática consiste en "la copia y/o reproducción no autorizada de datos o programas informáticos protegidos, así como la copia y/o reproducción o transmisión no autorizada por vía informática o telemática de cualquier otra obra u objeto protegido por los derechos de propiedad intelectual, con ánimo de lucro y en perjuicio del autor o del titular del derecho de explotación del mismo".¹²⁷

11.5 Sabotaje informático

El sabotaje informático consiste, básicamente, en borrar, suprimir o modificar sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema. La técnica más conocida para cometer este tipo de actividad es la que conocemos comúnmente con el nombre de "virus informático".

Un virus es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa. Se instala, se produce y causa diversos daños. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, pero también existen aquellos que pueden llegar a eliminar el contenido de una base de datos.

¹²⁷ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. p. 220.

Entre los virus más conocidos tenemos, a modo de ejemplo:

- Gusanos. Se fabrican de forma análoga a los virus, se infiltran en los programas ya sea para modificar o destruir los datos, pero se diferencian de los virus porque éstos no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo, un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego destruirse.
- Rutinas cáncer. Son aquellas que distorsionan el funcionamiento del programa y se auto reproducen al estilo de las células orgánicas alcanzadas por un tumor maligno.
- Bomba lógica o cronológica. Consiste en la introducción en un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha o circunstancia, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo. Las bombas lógicas son las que pueden resultar más dañinas y son difíciles de prever y detectar antes de que exploten, cuando el delincuente ya se encuentre lejos. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla.

Marchena Gómez señala que el sabotaje informático se refiere a aquella conducta consistente en la destrucción o en la producción generalizada de daños, datos, programas o documentos informáticos o telemáticos.¹²⁸

Morant Vidal apunta que el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas. Menciona que una de sus versiones más extendidas son las bombas lógicas, entendiendo por tales, el software, rutinas o modificaciones de programas que producen cambios, borrado de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador.¹²⁹

¹²⁸ Marchena Gómez, M. "El sabotaje informático: entre los delitos de daños y desórdenes públicos", en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, p. 356.

¹²⁹ Morant Vidal, J. *Protección penal de la intimidad...*, op. cit., pp. 46-47.

Asimismo, manifiesta que como principales características se pueden apuntar las siguientes:

- El tipo de actuación es retardada.
- El creador es consciente, en todo momento, del posible daño que puede causar y del momento en que éste se puede producir.
- Este ataque está determinado por una condición que determina el creador dentro del código.
- El código no se replica.
- Los creadores de este tipo de códigos malignos suelen ser personal interno de la empresa que, por discrepancias con la dirección o descontento, suelen programarlos para realizar el daño.

También sostiene que otra modalidad muy conocida de sabotaje lo constituyen los virus informáticos, que deben su nombre a su peculiaridad de reproducirse y transmitir sus efectos dañinos a una pluralidad de programas. Los virus consisten en programas que contienen una secuencia de efectos previsibles, que pueden reproducirse en la memoria del ordenador y contagiar a otros sistemas sirviéndose de los dispositivos de transferencia de datos sobre los que operan, o con los que se hallan conectados.

Corcoy Bidasolo señala que, dentro de los métodos de sabotaje informático, se suelen distinguir entre aquellos causados por sujetos extraños a la empresa o administración pública de que se trate, de aquellos otros realizados por los propios empleados del empresa:

- a) Los sabotajes informáticos causados por extraños a la empresa, en general, obedecen a móviles políticos y consisten en el incendio o la colocación de explosivos en los edificios donde se encuentran los sistemas informáticos.
- b) Los sabotajes informáticos ejecutados por los empleados de la propia empresa afectada se producen, normalmente, en caso de conflictos laborales o sociales dentro de la compañía o administración pública perjudicada.¹³⁰

¹³⁰ Corcoy Bidasolo, M. "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en Mir Puig, S. (comp.), *Delincuencia informática*, Editorial PPU, Barcelona, 1992, pp. 147-148.

Rovira del Canto señala que el sabotaje informático consiste en aquella "acción dirigida a la destrucción, inutilización, o incapacitación de sistemas informáticos y telemáticos, o de datos o información contenida, transferida o transmitida de los mismos, así como de sus funciones de procesamiento y tratamiento, bien mediante la utilización de métodos lógicos, informáticos o telemáticos, bien mediante el abuso de los equipos físicos".¹³¹

De la misma manera, señala que una de las formas más conocidas para cometer este tipo de actividades son las llamadas bombas lógicas, los gusanos y los virus informáticos, y define los virus informáticos como programas que se extienden por los sistemas informáticos, en algunos casos con efectividad o activación retardada en el tiempo, y que causan daños y perjuicios en el sistema o equipo, menciona que estos programas son distribuidos normalmente a través de la piratería de software y por el uso de redes informáticas.

A manera de conclusión, podríamos decir que este tipo de delincuencia, a últimas fechas, se ha puesto de moda, ocasionando a millones de personas y de empresas un sinnúmero de daños en sus equipos y sistemas, siendo éstos en algunos casos muy graves, por lo que es necesario una buena regulación que sancione esta conducta ilícita. Por último y como señala Marchena Gómez:

[...] la capacidad destructiva al alcance de cualquier cracker puede llegar a resultar ilimitada. La inoculación de virus informáticos en sistemas interconectados y el empleo de técnicas de bombardeo de datos, valiéndose de computadoras esclavizadas, permiten multiplicar hasta el infinito el potencial número de afectados. El riesgo de daños a gran escala, asociados al simple envío de un programa destructivo, se cierne sobre los numerosos usuarios de Internet. Con una periodicidad cada vez más regular la red se ve asaltada por la amenaza de un virus que, burlando todos los filtros y barreras defensivas hasta ese momento ideados, propaga sus devastadores efectos a lo largo y ancho de las redes telemáticas.¹³²

11.6 Fraude informático

Por lo que hace al fraude informático podemos decir que éste consiste en cualquier conducta y/o manipulación realizada a través o por

medio de un sistema informático, con el objeto de obtener un beneficio ilegítimo, ocasionando un perjuicio a una o varias personas.

De esta manera mencionaremos lo que, para algunos autores, es el fraude informático o también llamado estafa informática. Así, para Romeo Casabona, el fraude informático se equipara a la manipulación de datos informatizados, y lo define como "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o están ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero".¹³³

Corcoy y Joshi señalan que las estafas por computador son "las manipulaciones del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, con la intención de obtener un beneficio económico, causando a un tercero un perjuicio patrimonial".¹³⁴

Por otro lado Camacho Losa define al fraude informático como "toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito".

Por último, Moránt Vidal¹³⁵ señala que entre los supuestos más frecuentes de estas conductas se pueden citar los siguientes:

- a) Daños engañosos, que hace referencia a las distintas formas de alteración de los datos contenidos en el ordenador antes o durante su proceso informático. En la mayor parte de los casos, este supuesto se traduce en manipulaciones del ordenador tendientes a introducir informaciones falsas, o a eliminar aquellas que son verdaderas.
- b) Caballo de Troya. Consiste en introducir rutinas por instrucciones aparentemente inocuas o incluso inútiles, que distorsionan el funcionamiento de los sistemas informáticos. En la mayor parte de los casos implican la introducción de un conjunto de instrucciones para que el ordenador lleve a cabo operaciones no autorizadas, por ejemplo, transferir fondos a la cuenta bancaria del delincuente.

¹³¹ Rovira del Canto, E. Delincuencia informática y fraudes informáticos..., op. cit., p. 225-237.

¹³² Marchena Gómez, M. El sabotaje informático..., op. cit., pp. 356-357.

¹³³ Romeo Casabona, C.M., Poder Informático y Seguridad Jurídica..., op. cit., p. 47.

¹³⁴ Corcoy Bidasolo, M. y Joshi Jubert, U. Delitos contra el patrimonio..., op. cit., p. 141.

¹³⁵ Morant Vidal, J. Protección penal de la Intimidad..., op. cit., pp. 46-47.

c) La técnica del salami, que permite sustraer mediante redondeo pequeñas cantidades de activos financieros de diversas cuentas bancarias para situar su monto total, que puede ascender a cantidades considerables en la cuenta del delincuente.¹³⁶

¹³⁶ Camacho Losa, L., *El delito informático...*, op. cit., p. 28.

CAPÍTULO XII

Delitos informáticos en el código penal español

A continuación mencionaré algunas conductas delictivas que están reguladas en la legislación española. Se trata de delitos que afectan todo tipo de bienes jurídicos y que sólo tienen en común el hecho de poderse cometer por medios informáticos y, en muchos casos, por Internet.

12.1 Delitos contra la libertad: amenazas y coacciones

La forma de comisión más habitual es mediante e-mail (anónimo o no), algo que se ve favorecido por el anonimato que permiten los llamados remailers anónimos y los cibercafés, dificultando enormemente a las fuerzas de seguridad su persecución.

Los artículos 169 y siguientes del Código Penal regulan los diferentes tipos de amenazas. El artículo 169 del Código Penal castiga la conducta de aquel que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el c den socioeconómico. La pena es de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de seis meses a tres años.

Las penas indicadas se elevan si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

12.2 Delitos contra la libertad sexual

El más claro ejemplo de estos delitos cometidos a través de Internet es la pornografía infantil, que apareció en el Código Penal español en 1999. Las siguientes conductas serán castigadas con pena de prisión de uno a tres años:

- a) El que utilizare a menores de edad o incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, o financiare cualquiera de estas actividades.
- b) El que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere origen en el extranjero o fuere desconocido. A quien poseyera dicho material para la realización de cualquiera de estas conductas se le impondrá la pena en su mitad inferior.

Se castiga con la pena superior en grado cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

Debe destacarse, en lo que se refiere a estos delitos, que la pena es exclusivamente por la distribución de la pornografía. A aquellos que hayan participado en los abusos de menores se les castiga además con las penas correspondientes al delito sexual cometido. Y en tal caso no estamos hablando de delito informático, sino de algo mucho más grave.

12.3 Delitos contra la intimidad: descubrimiento y revelación de secretos

La Constitución Española de 1978 protege el derecho a la intimidad en su art. 18.4 CE emplazando al legislador para que lo desarrolle con una Ley posterior. Así lo hizo mediante la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD). Aparte de esta Ley también el Código Penal (Español) protege la intimidad en el art. 197 CP. La intimidad

puede entenderse, según Muñoz Conde,¹³⁷ como un derecho de control sobre la información y los datos de la otra persona, incluso sobre los ya conocidos, para que sólo puedan utilizarse conforme a la voluntad de su titular.

Las nuevas tecnologías cada vez se van implantando más en nuestra sociedad, hasta el punto en que se ha hecho indispensable para determinadas tareas de vital importancia el uso de la informática y las telecomunicaciones, y además proporcionan un gran servicio a toda la sociedad. Aparte de esto que se ha expuesto, seguro que a cualquier persona se le puede ocurrir un buen número de beneficios que las nuevas tecnologías proporcionan; pero como cualquier cosa en este mundo tiene sus aspectos negativos, y en este sentido la informática y las telecomunicaciones son utilizadas para atacar uno de los bienes fundamentales constitucionalmente reconocidos de cualquier persona: la intimidad. La informática se ha convertido en el medio propicio para atentar contra la intimidad de las personas, ya sea por simple entretenimiento (hackers), o con fines lucrativos; de cualquiera de las dos formas la intimidad de una persona se ve afectada.

Por todo ello, el legislador ha de regular una realidad social, y penar determinadas conductas lesivas de ciertos bienes fundamentales de la persona. Entre otras leyes tenemos el Código Penal (español) de 1995, el cual dedica el Título X del Libro II a los delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio, aunque sólo nos interesan los preceptos referentes a los delitos contra la intimidad, y en concreto los que usen medios informáticos para ello.

El artículo 197 del Código Penal establece una pena de prisión de uno a cuatro años y multa para el que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.

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

¹³⁷ Muñoz Conde, F. Derecho penal. Parte Especial, Editorial Tirant lo Blanch, Valencia, 2002, p. 249.

ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Igualess penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien utilice en perjuicio del titular de los datos a un tercero.

Las penas se ven incrementadas cuando quien revela el secreto es el que está a cargo de los archivos (caso de los administradores maliciosos), cuando se revelan a terceros, cuando afecten a datos de carácter personal que revelen la ideología, religión, ciencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz o en casos de cesión a terceros de secretos.

Por un lado, tenemos el art. 197.1 CP donde se contempla el tipo básico de descubrimiento de secretos, que consiste en apoderarse de secretos para descubrir, sin una posterior divulgación o publicidad. La jurisprudencia ha entendido por apoderamiento la aprehensión u obtención ilícita, así como la retención de lo recibido por error.

Pero, ¿qué se entiende por secreto?, es "el conocimiento reservado a un número limitado de personas, y oculto a otras"; secreto será pues todo conocimiento reservado, que el sujeto activo no conozca, o no esté seguro de conocer, y que el sujeto pasivo no quiera que se conozca; pero no hemos de confundir el secreto con el objeto en el que materializa, que puede ser un papel, una carta, mensajes de correo electrónico o cualquier otro documento personal. También hemos de tener presente que cuando los documentos afecten a la seguridad nacional, nos hemos de remitir a lo regulado en los arts. 583.3 y 584 CP, que prevén penas de doce a veinte años, y de seis a doce años, respectivamente. Además, cuando se trate de secretos de empresa, se debe tener presente lo dispuesto en los arts. 278 y 279 del CP.

Por otro lado, tenemos el art. 197.2 CP. En éste el objeto material sobre el que ha de recaer la conducta típica son "datos de carácter personal o familiar ajenos". La conducta típica que se recoge en este artículo puede ser tanto apoderarse, utilizarse o modificar, en perjuicio de tercero, es decir, toda acción de tomar, coger, o poner bajo su poder o control, por ejemplo, copiar.

El último inciso hace referencia a "acceder por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero". Vemos que las conductas típicas son acceder, alterar o utilizar, pero ya no datos reservados, sino "ficheros o soportes

informáticos, electrónicos, o telemáticos". En resumen este artículo castiga básicamente el "hacking", esto es, acceder a un sistema, sin estar autorizado para ello, y visualizar los datos de éste. Además, se pueden dar otras conductas, como puede ser aprovecharse de esa información y alterar, modificar, cambiar o vaciar la información que el sistema vulnerado contenía. La pena con que se sanciona estas conductas es prisión de uno a cuatro años, y multa de doce a veinticuatro meses, al igual que el art. 197.1 CP.

Incluso el legislador ha previsto otro tipo agravado, el del art. 197.4 CP, si los hechos descritos en el tipo básico los realizan "las personas encargadas o responsables" de los ficheros, soportes, archivos o registros. Con ello vemos que la agravación (prisión de tres a cinco años, si se realiza la conducta de los párrafos 1 y 2 del art. 197 CP, y prevé la pena en su mitad superior si verifica la conducta del párrafo 3 del mismo artículo del CP) se produce por una especial circunstancia del sujeto activo. Por supuesto hemos de delimitar el concepto de "personas encargadas o responsables", y para ello lo debemos hacer de forma restrictiva, es decir, sólo serán encargados o responsables las personas que, en virtud de una disposición legal o contractual, posean esa condición, por ejemplo, el administrador del sistema, que normalmente es responsable en virtud de un contrato.

Por otro lado en el Código Penal, en su art. 197.5, se prevé otra agravación en función del contenido de los datos descubiertos, y en concreto cuando se traten de datos "sensibles", que son los referentes a la "ideología, religión, creencias, salud, origen racial o vida sexual". La agravación se produce porque tiene un mayor contenido de injusto el vulnerar la intimidad en sus vertientes más fundamentales y elementales.

Otra figura cualificada es la contenida en el art. 197.6 CP, donde se prevén penas superiores cuando las conductas descritas en el tipo básico se realicen con "ánimo de lucro", y a su vez distingue la punición dependiendo de si los datos son "sensibles" (art. 197.5 CP), o no lo son. El artículo 197 equipara a todos los efectos el e-mail al correo tradicional, estableciendo idéntica pena.

Los secretos a los que se refiere el artículo 197 son siempre secretos de personas físicas. Cuando hablamos de secretos de empresa, su revelación no se castiga como delito contra la intimidad, sino como delito contra el mercado que atenta contra las personas.

También hemos de tener presente que, cuando los documentos afecten a la seguridad nacional, nos hemos de remitir a lo regulado en los arts. 583.3 y 584 CP, que prevén penas de doce a veinte años, y de seis a doce años, respectivamente. Además, cuando se trate de secretos de empresa, se ha de tener presente lo dispuesto en los arts. 278 y 279 del CP.

12.4 Delitos contra el honor: calumnia e injuria

El artículo 205 define como calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad. La injuria se define en el artículo 208 como la acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Un ejemplo de esto en Internet se da a través de los foros públicos: se insulta, se suplanta la personalidad de otro, y en ocasiones se llegan a realizar ofertas sexuales poniéndolas en nombre de otra persona.

Delitos contra el patrimonio y el orden socioeconómico

Estafa Informática

Con la ayuda de las nuevas tecnologías aparecen nuevos delitos y nuevas formas de comisión de delitos. Ante esto, el legislador no se puede quedar de brazos cruzados y no regular este aspecto de la informática, y así ha sido. Un ejemplo claro de esto es la introducción de la estafa informática en el Código Penal, que no es otra cosa que una estafa cometida usando medios informáticos; y así se regula en dicho texto legal:

Art. 248. 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 patrimonial en perjuicio de tercero.

Este artículo está regulando una estafa normal y corriente, excepto que aquí no se engaña, ya que a una máquina no se le puede engañar, esto sólo se puede hacer a los humanos.

Obviamente como en cualquier otra estafa ha de haber un ánimo de lucro, la transferencia no consentida de cualquier activo patrimonial, y el perjuicio de un tercero.

El ánimo de lucro ha de ser entendido como la intención de obtener un enriquecimiento patrimonial correlativo al perjuicio ocasionado.

Para que se dé la estafa ha de haber una transferencia no consentida de un activo patrimonial, en forma de entrega, cesión o prestación de la cosa, derecho o servicio. Por último, ha de existir un perjuicio para un tercero.

Para que exista delito de estafa la suma de lo defraudado ha de superar las cincuenta mil pesetas, de lo contrario sería una falta de estafa regulada en el art. 623.4 CP donde se prevé un arresto de seis fines de semana o multa de uno a dos meses; mientras que el delito de estafa informática está castigado con la pena de prisión de seis meses a cuatro años, obviamente cuando exceda las cincuenta mil pesetas, y cumpla todos los requisitos del art. 248.2 CP.

Defraudaciones de fluido

El artículo 255 del Código Penal dispone pena de multa para el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluidos ajenos, por alguno de los medios siguientes:

1. Valiéndose de mecanismos instalados para realizar la defraudación.
2. Alterando maliciosamente las indicaciones o aparatos contadores.
3. Empleando cualesquiera otros medios clandestinos.

Asimismo, el artículo 256 establece que el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Delitos contra la propiedad intelectual

Según la Ley de propiedad intelectual, ésta se compone de derechos de carácter personal y patrimonial que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas por la ley.

Según esta definición la propiedad intelectual se compone de un aspecto moral y otro patrimonial. Lo patrimonial lo vemos reflejado

en el art. 270 CP, cuando hace referencia de forma expresa al ánimo de lucro del sujeto activo. Sin embargo, el contenido moral no aparece por ningún lado en el Código Penal, el cual se ve dañado cuando se realiza la conducta típica.

De acuerdo con el art. 1 de la Ley de propiedad intelectual, la propiedad intelectual es del autor de la obra por el mero hecho de haberla creado él, con lo que la inscripción registral no es necesaria para que se realice el tipo del art. 270 CP. Por otro lado, hemos de tener en cuenta, según el art. 270 CP, que el consentimiento del autor excluye el tipo.

La conducta descrita en el art. 270 CP se ve agravada por las circunstancias previstas en el art. 271 CP, que son: la especial trascendencia del beneficio económico y la especial gravedad del daño causado. Cuando se da alguna de estas circunstancias la pena se agrava, en concreto se pasa de la pena de prisión de seis meses a dos años (tipo básico), a prisión de un año a cuatro años (tipo agravado). Para determinar la gravedad del daño causado es necesario acudir a la Ley de propiedad intelectual.

Según el Código Penal, además de la respectiva pena, el Juez puede decretar también el cierre provisional o definitivo del local, industria o establecimiento del condenado.

Las conductas descritas en el art. 270 CP son reproducir, plagiar, distribuir, comunicar, importar y exportar obras literarias, artísticas o científicas, sin la autorización de los titulares de los derechos de propiedad intelectual.

Es importante mencionar el tercer párrafo del art. 270 CP, ya que castiga expresamente la tenencia o fabricación de mecanismos que vulneren la protección de los programas informáticos, es decir, con base en este artículo es ilegal tener o fabricar programas para "crackear" otros programas.

Delitos contra la propiedad industrial

La propiedad industrial es un derecho sobre un bien inmaterial. Son bienes capaces de ser transformados en un bien material y físico, el cual puede ser transmitido, poseído, utilizado, etc.

La regulación y protección de la propiedad industrial en el Código Penal se encuentra en los arts. 273 a 277, que se ven completados por la Ley de patentes de invención y modelos de utilidad de 1986, y la Ley de marcas de 1988.

Lo que se trata proteger con estos artículos es el derecho a la utilización reservada de determinados objetos: la explotación exclusiva de un invento u objeto (art. 273 CP); un signo registrado, ya sea de una marca, un nombre comercial, o un rótulo de establecimiento (art. 274 CP); o de una denominación de origen, o indicación geográfica representativa de una determinada calidad (art. 275 CP).

En cualquiera de los casos anteriormente mencionados el objeto, logotipo, etc., ha de estar registrado conforme a la Ley de marcas, en caso contrario no hay protección alguna, en base al Código Penal.

Delitos relativos al mercado y los consumidores

Algunos de los más comunes que podemos encontrar, como el espionaje industrial, se encuentran regulado en el artículo 278 CP, estableciéndose la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses para el que, para descubrir un secreto de empresa se apodereare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197 CP. La pena se incrementa para el caso de divulgación de secretos y para cuando intervienen personas obligadas contractualmente a guardarlos.

Y, por otro lado, el uso de información privilegiada que se encuentra regulado en el artículo 285 CP, que a la letra dice, "quien en forma directa o por persona interpuesta usare de alguna información relevante para la cotización de cualquier clase de valores o instrumentos negociados en algún mercado organizado, oficial o reconocido, a la que haya tenido acceso reservado con ocasión del ejercicio de su actividad profesional o empresarial, o la suministrarle obteniendo para sí o para un tercero un beneficio económico superior a setenta y cinco millones de pesetas o causando un perjuicio de idéntica cantidad, será castigado con la pena de prisión de uno a cuatro años y multa de tanto al triple del beneficio obtenido o favorecido". Será un delito informático únicamente en la medida que para su comisión se haga uso de la información a través de Internet.

Falsedades

Dentro de las falsedades podemos encontrar que, en el artículo 387 CP, se equipara a las tarjetas de crédito con papel moneda y moneda

metálica, esto trae como consecuencia que se pueda penar la fabricación de tarjetas de crédito falsas. Y, por otro lado, el artículo 26 CP, considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica. En lo referente a Internet podemos encontrar esto en la firma electrónica que, con el cada vez más frecuente uso de ésta, veremos que los delincuentes se las ingeniarán para cometer conductas delictivas.

12.6 Virus informáticos

El artículo 264.2 del Código penal español establece pena de prisión de uno a tres años y multa de doce a veinticuatro meses al que, por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este tipo penal es aplicable en los casos de introducción maliciosa de virus, así como en los de hacking destructivo. A priori la creación de un virus no está contemplada como delito en el Código penal español. Su introducción en sistemas informáticos, directamente o a través de Internet sí puede ser delictiva, en función de las consecuencias del virus. En este sentido, habría que diferenciar entre:

Virus inocuos: aquellos que sólo expanden información, sin dañar ni ralentizar sistemas informáticos.

Virus como herramienta de hacking: su diseño como virus está destinado a introducirse en los sistemas, no para dañarlos, sino para obtener información como contraseñas, topología de redes, o para crear cuentas de usuario.

Si estos virus son introducidos en un sistema y se obtiene información secreta, se castigaría como revelación de secretos o como espionaje internacional, para el caso de que fueran secretos de empresa.

Virus como herramienta de estafa: son aquellos destinados al fraude electrónico, que consiguen transferencias de activos, defraudando a empresas y banca online, así como mediante operaciones fraudulentas en Bolsa.

Virus destructivos: Serían aquellos cuya finalidad es la destrucción o alteración de la información contenida en sistemas informáticos.

Sólo para este caso de virus se podría hablar estrictamente de daños informáticos. La simple autoría del virus no está penada, salvo que pueda probarse que el creador actuó en conveniencia con los distribuidores del mismo. En cuanto a éstos, serán castigados por aquellos hechos en los que intervenga dolo directo: debe existir la intencionalidad de dañar, robar secretos, estafar o causar daños a una empresa en concreto, o aprovecharse de los resultados en caso de infección discriminada. La difusión imprudente sólo puede pensarse cuando los daños superan los 10 millones de pesetas, de acuerdo con el artículo 267 del Código Penal.



Vanguardia en
Ciencias Penales

Instituto de Formación Profesional

Biblioteca

CAPÍTULO XIII

Delitos informáticos en la legislación mexicana

13.1 Legislación en materia penal en México

La Constitución Política Mexicana establece la organización del país bajo un sistema federal, dividido en varios Estados, cada uno de los Estados tiene su propio Código Penal y su Código de Procedimientos Penales, al igual que un Código Penal Federal y Código Federal de Procedimientos Penales para todos aquellos delitos de carácter federal, y en los que única y exclusivamente tiene competencia la Federación.¹³⁸

Los tribunales de la federación son competentes para conocer, entre otras materias (artículo 104, fracciones I, II, III y VI de la Constitución mexicana),¹³⁹ de las controversias de orden civil y criminal que se sus-

¹³⁸ Artículo 18 párrafo 2º «Los Gobiernos de la Federación y de los Estados organizarán el sistema penal, en sus respectivas jurisdicciones».

¹³⁹ Artículo 104 «Corresponde a los tribunales de la Federación conocer:

I.- De todas las controversias del orden civil o criminal que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado Mexicano. Cuando dichas controversias sólo afecten intereses particulares, podrán conocer también de ellas, a elección del actor, los jueces y tribunales del orden común de los Estados y del Distrito Federal. Las sentencias de primera instancia podrán ser apelables ante el superior inmediato del juez que conozca del asunto en primer grado;

II.- De todas las controversias que versen sobre derecho marítimo;

III.- De aquéllas en que la Federación fuese parte;

[...]

citen sobre el cumplimiento y aplicación de leyes federales o con motivo de los tratados celebrados con potencias extranjeras.¹⁴⁰ Los delitos del orden federal se establecen en el Código Penal Federal o con alguna aplicación federal, tal como sucede en el Código del Procedimiento Electoral, Ley de la Propiedad Intelectual e Industrial, Ley Federal contra la Delincuencia Organizada, Ley para la Protección del Medio Ambiente, Ley para Prevenir la Discriminación y los Delitos Fiscales, entre otros.

La conducta típica puede ser realizada por servidores públicos o particulares, pero el ilícito debe estar tipificado en leyes de índole federal o cometidos en zonas señaladas como federales, por ejemplo, caminos públicos o zonas de abastecimiento de energía. Del mismo modo, pueden ser delitos cometidos por particulares, pero que afecten los intereses de la federación, catalogados por la gravedad del interés y el bien jurídico tutelado.

Por otra parte, es importante hacer una distinción entre las leyes de carácter nacional y las leyes que tienen su origen fuera del territorio nacional, y que por su naturaleza se pueden aplicar en el país y a sus ciudadanos. En Derecho Positivo mexicano, la Constitución Política de los Estados Unidos Mexicanos señala la jerarquía de las normas jurídicas (estableciendo en sí misma que no existe Ley suprema a la propia Constitución) que se aplican en territorio nacional y/o a los nacionales y se transcribe a continuación el artículo:

Artículo 133.

Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados.

Así, de conformidad con el citado artículo 133 de la Constitución Política de los Estados Unidos Mexicanos, la jerarquía de las normas

VI.- De los casos concernientes a miembros del Cuerpo Diplomático y Consular».

¹⁴⁰ En cada sistema nacional se determinan los órganos competentes para dirigir y autorizar la negociación de los tratados. De ordinario, ésta es una facultad del Poder ejecutivo que se atribuye genéricamente al Jefe del Estado como titular del "poder exterior". Se ejerce, por delegación de éste, por el órgano central (Gobierno) y un departamento específico, el de Asuntos Exteriores, que es el órgano de Gobierno encargado de todos los asuntos de carácter internacional.

jurídicas en México coloca a la propia Constitución por arriba de los demás ordenamientos jurídicos.

13.2 La acción penal en México

La palabra acción proviene de "actio" que es su acepción gramatical y que significa toda actividad o movimiento que se encamina a un determinado fin, la misma Real Academia de la Lengua Española define a la acción desde una concepción jurídica como: «En sentido procesal, derecho a acudir a un juez o tribunal recabando de él la tutela de un derecho o de un interés». Para Florian la acción penal es el poder jurídico de excitar y promover la decisión del órgano jurisdiccional sobre una determinada relación de derecho penal. La acción penal domina y da carácter a todo el procedimiento, lo inicia y lo hace avanzar hasta su meta. La acción penal nace con el delito y la acción procesal penal se inicia cuando se motiva una serie de acciones y de actividades ante el órgano jurisdiccional, con la finalidad de que se declare una resolución por parte de la autoridad competente en el caso concreto, extinguiéndose cuando cesan esas actividades. Otra definición de acción penal, y que a mi parecer es más completa, la define Arilla Bas como, "el poder jurídico del propio Estado de provocar la actividad jurisdiccional con objeto de obtener el órgano de ésta una decisión que actualice la punibilidad formulada en la norma respecto de un sujeto ejecutor de conducta descrita en ella".¹⁴¹

La acción penal es, en términos generales, de condena, pero al mismo tiempo declarativa, puesto que se interesa a obtener la declaración de la responsabilidad penal. El periodo de la preparación de la acción procesal principia en el momento de la presentación de la denuncia o querrela por comisión de un hecho ilícito y termina con la consignación de la averiguación previa ante un juez penal, por lo que la acción procesal penal como tal, nace con la determinación judicial del Auto de formal prisión,¹⁴² que es concretamente la sujeción del procesado al proceso penal en sí mismo, ya que en la fase persecutoria se desarrolla y en la acusatoria haya su plenaria acusación.¹⁴³

¹⁴¹ Arilla Bas, F. El procedimiento penal en México, editorial Porrúa, México, 1997. p. 26.

¹⁴² El Auto de formal prisión que tiene su fundamento en el artículo 19 Constitucional y tiene un parentesco de ascendencia con la figura española del conocido Auto de procesamiento, el cual ofrece puntos de conexión precisos con el Auto de formal prisión del régimen mexicano.

¹⁴³ Colín Sánchez, G. Derecho mexicano de procedimientos penales, editorial Porrúa, México, 1979. p. 232.

13.3 Los delitos informáticos en la legislación mexicana

En la legislación mexicana encontramos un gran rezago del tema de los delitos informáticos. Mientras que en otros países es constantemente revisado y actualizado, en México, a pesar de que lleva 10 años incluido en la legislación, poco más se ha hecho.

Es importante hacer el señalamiento que desgraciadamente en México no existe una clara toma de conciencia respecto de la necesidad de regular los delitos que contengan cuestiones relacionadas con la informática, a pesar de que hace una década el Diario Oficial de la Federación, el 17 de mayo de 1999, incluyó por primera vez figuras relacionadas con esta materia. Entonces se consideró a México un país de avanzada en este sentido, pues hasta ese momento pocos países consideraban estas figuras como una prioridad. Sin embargo, también es importante destacar que desde entonces no ha habido sino pequeños señalamientos a artículos precisos dentro de las distintas legislaciones (en materia federal y materia local de los distintos Estados). Es necesario reconocer que la tecnología nos ha rebasado, que las legislaciones federales y locales no han cubierto las necesidades que la sociedad demanda y que para entablar una lucha frontal es necesario actualizar el marco normativo en este tenor.

Empezaremos por hacer un breve recorrido por la legislación federal, de las distintas leyes que hacen referencia a cuestiones en las que se consideran los delitos informáticos, de aquellas actividades que son realizadas a través de una computadora o que son el medio comisivo para la realización del mismo. Posiblemente la primera por su importancia pueda ser la Ley Federal contra la Delincuencia Organizada, que engloba una gama considerable de acciones que pueden ser cometidas mediante un ordenador y que constantemente se actualizan con tecnología de punta. (El énfasis en las siguientes citas es mío.)

Ley Federal contra la Delincuencia Organizada

Artículo 2o.- Cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras, tienen como fin o resultado cometer alguno o algunos de los delitos siguientes, serán sancionadas por ese sólo hecho, como miembros de la delincuencia organizada:

- I. Terrorismo, previsto en los artículos 139 al 139 Ter y terrorismo internacional previsto en los artículos 148 Bis al 148 Quáter; contra la salud, previsto en los artículos 194 y 195, párrafo primero; falsificación o alteración de moneda, previstos en los artículos 234, 236 y 237; operaciones con recursos de procedencia ilícita, previsto en el artículo 400 Bis; y el

previsto en el artículo 424 Bis, todos del Código Penal Federal;

- II. Acopio y tráfico de armas, previstos en los artículos 83 bis y 84 de la Ley Federal de Armas de Fuego y Explosivos;
 - III. Tráfico de indocumentados, previsto en el artículo 138 de la Ley General de Población;
 - IV. Tráfico de órganos previsto en los artículos 461, 462 y 462 bis de la Ley General de Salud;
 - V. Corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo previsto en el artículo 201; Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en el artículo 202; Turismo sexual en contra de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en los artículos 203 y 203 Bis; lenocinio de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, previsto en el artículo 204; asalto, previsto en los artículos 286 y 287; secuestro, previsto en el artículo 366; tráfico de menores o personas que no tiene capacidad para comprender el significado del hecho, previsto en el artículo 366 Ter, y robo de vehículos, previsto en los artículos 376 Bis y 377 del Código Penal Federal, o en las disposiciones correspondientes de las legislaciones penales Estatales o del Distrito Federal, y
- Fracción reformada DOF 27-03-2007, 27-11-2007, 23-01-2009
- VI. Trata de personas, previsto y sancionado en los artículos 5 y 6 de la Ley para Prevenir y Sancionar la Trata de Personas.

Como se puede observar, en la legislación relativa a la delincuencia organizada en materia federal, no existe un señalamiento específico a los delitos cometidos a través de medios informáticos. Sin embargo, se puede inferir de lo que se señala en la fracción V del citado artículo 2º cuando hace mención a la pornografía infantil y los medios de transmisión de la misma. Considero fundamental determinar que es precisamente la delincuencia organizada la que utiliza tecnología de punta para la distribución y comercialización de sus productos, y que muchas veces los Estados no pueden alcanzar la velocidad con la que se mueven estos grupos criminales.

La preocupación sobre esta evolución de la delincuencia tradicional a la tecnológica no ha sido ajena a las instituciones. Uno de los principales problemas, y del que es plenamente conocedora la delincuencia

organizada, radica en la extraterritorialidad del delito. Una actividad con origen en un país determinado puede verse replicada y surtir efecto en decenas de países terceros, con los que puede que ni siquiera existan tratados de cooperación policial o judicial de ninguna índole. Pero, en el caso de que los hubiera, la escasa cuantía de estos fraudes rara vez propicia la emisión de órdenes judiciales internacionales que permitan la captura del delincuente y mucho menos la restitución del daño.

Código Penal Federal

En relación al Código Penal Federal también encontramos diversos artículos que hacen especial mención de los delitos cometidos a través de nuevas tecnologías pero, como ya se ha señalado, seguimos con un rezago legislativo que impide a la autoridad actuar con eficiencia.

Artículo 167.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:

[...]

VI.- Al que dolosamente o con fines de lucro interrumpa o interfiera las comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;

Artículo 177.- A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Estos dos tipos penales establecidos en los artículos 167 y 177 hacen mención a las figuras en materia federal de vías de comunicación y correspondencia, y en los que se señala los tipos de comunicación que pueden ser intervenidas, y en las que se contempla el uso de tecnologías para su intervención. Aclarando en el artículo 177 que para que puedan ser efectuadas es necesario que exista una orden judicial previa, ya que de lo contrario se estará cometiendo un delito.

Artículo 201.- Comete el delito de corrupción quien obligue, induzca, facilite o procure a una o varias personas menores de 18 años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo a realizar cualquiera de los siguientes actos:

[...]

f) Realizar actos de exhibicionismo corporal o sexuales simulados o no, con fin lascivo o sexual. A quien cometa este delito se le impondrá: en el caso del inciso a) o b) pena de prisión de cinco a diez años y multa de quinientos a

mil días; en el caso del inciso c) pena de prisión de cuatro a nueve años y de cuatrocientos a novecientos días multa; en el caso del inciso d) se estará a lo dispuesto en el artículo 52, del Capítulo I, del Título Tercero, del presente Código; en el caso del inciso e) o f) pena de prisión de siete a doce años y multa de ochocientos a dos mil quinientos días.

Cuando se trate de mendicidad por situación de pobreza o abandono, deberá ser atendida por la asistencia social.

No se entenderá por corrupción los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre función reproductiva, la prevención de enfermedades de transmisión sexual y el embarazo de adolescentes, siempre que estén aprobados por la autoridad competente; las fotografías, video grabaciones, audio grabaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares.

En caso de duda el juez solicitará dictámenes de peritos para evaluar la conducta en cuestión. Cuando no sea posible determinar con precisión la edad de la persona o personas ofendidas el juez solicitará los dictámenes periciales que correspondan.

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

México es considerado el segundo país con mayor producción de pornografía infantil en Latinoamérica. “La pornografía infantil constituye un problema de dimensión internacional que se ha facilitado con la entrada de nuevas tecnologías”. La pornografía infantil es un delito que deja huellas permanentes en las víctimas e impide su sano desarrollo psicológico, por lo que las autoridades mexicanas deben incrementar su combate. Varios países y organizaciones europeas han aprobado medidas para reforzar la seguridad en Internet, entre las que destaca la Declaración de Praga, la cual combate las actividades ilegales en Internet y la propagación de pornografía infantil.

Por otro lado tenemos una figura de reciente creación que se denomina el ‘sexting’, un juego de palabras en inglés con los términos ‘sex’ y ‘texting’, se ha convertido en una preocupación para padres y colegios a nivel internacional con la proliferación de teléfonos móviles con cámaras y sitios de redes sociales, pero esas imágenes pueden ser calificadas de pornografía infantil por la ley. En Estados Unidos, una encuesta mostró el pasado año que uno de cada cinco adolescentes dijeron que habían enviado o colgado en Internet fotografías de desnudos o semidesnudos de ellos mismos, y el 39% indicó que habían mandado o colocado mensajes sugerentes, según una campaña nacional para impedir embarazos no planeados y de adolescentes. En Estados Unidos se han iniciado varios procesos y una chica, de 18 años, se suicidó después de ser objeto de mofa cuando una foto suya enviada por SMS circuló por su escuela.

El delito de pornografía infantil señalado en los artículos 201 y 202 del Código Penal Federal hace referencia a estas figuras y sanciona a quienes cometan estos delitos en personas menores de 18 años o quienes no puedan comprender el hecho, pero las implicaciones de carácter social derivadas de esta situación conllevan una responsabilidad para todos los gobiernos de trabajar de manera conjunta para evitar la difusión de estos materiales a través de la Red.

Respecto a los delitos federales en materia de derechos de autor el Código Penal Federal establece concretamente lo siguiente:

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

- I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los

términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

- II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Ley Federal de Telecomunicaciones

Artículo 3. Para los efectos de esta Ley se entenderá por:

[...]

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

IX. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

X. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

[...]

XIV. Telecomunicaciones: toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos, u otros sistemas electromagnéticos.

La Ley Federal de Telecomunicaciones establece en el apartado anterior cuáles son los tipos de telecomunicaciones, qué es la red pública y la red privada, y brevemente describe cómo opera, pero sería conveniente que la propia Ley dicte las pautas necesarias para una adecuada regulación en materia de informática. El día 30 de abril de 2009 se publicó en el Diario Oficial de la Federación el Decreto que establece la reforma al artículo 73 Constitucional cuyo texto adiciona la fracción XXIX-O, otorgándole facultades al Congreso Mexicano para legislar en materia de protección de datos en posesión de los particulares. Lo más

peculiar de esta reforma es que el artículo segundo transitorio de ese Decreto obliga al propio Congreso de la Unión a expedir la ley en la materia en un plazo no mayor a 12 meses, contados a partir de la entrada en vigor del decreto, es decir antes del 30 de abril de 2010.

La publicación de este texto abrirá un campo de batalla entre las empresas que manejan y procesan datos personales, los ciudadanos y otros sectores vulnerables. Esta reforma tiene la posibilidad de habilitar un nuevo diálogo más abierto, concreto y organizado en el Congreso con la participación plena de representantes clave de todos los sectores de la sociedad mexicana y no solamente con los representantes del sector bancario, empresarial y de la industria de las telecomunicaciones e Internet como son la AMIPCI y CANIETI, que sólo han logrado retrasar las iniciativas en materia de protección de datos desde hace más de siete años y velar únicamente por sus intereses económicos, sin tomar en cuenta los derechos del individuo a la tutela y protección de sus datos personales.

Ley de Instituciones de Crédito

Artículo 112 Bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:

- I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;
- II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;
- III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;
- IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;
- V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o
- VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada.

Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

- I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o
- II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Artículo adicionado DOF 26-06-2008

Artículo 113 bis.- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito, se le aplicará una sanción de tres a diez años de prisión y multa de quinientos a treinta mil días de salario.

Si quienes cometen el delito que se describe en el párrafo anterior son funcionarios o empleados de las instituciones de crédito o terceros ajenos pero con acceso autorizado por éstas a los sistemas de las mismas, la sanción será de tres a quince años de prisión y multa de mil a cincuenta mil días de salario.

Los tipos señalados anteriormente y de que hace mención la Ley de Instituciones de Crédito han considerado reformar la legislación en la materia desde el año de 2004, ya que el desarrollo de las tecnologías de la información ha abierto las puertas a nuevas posibilidades de delincuencia. El acceso sin autorización (piratería informática), el sabotaje informático, la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos. A medida que ha aumentado la delincuencia cibernética, diversos países han publicado leyes declarando ilegales nuevas prácticas o han actualizado sus ordenamientos legales para que delitos tradicionales, incluidos el fraude, se consideren ilícitos en el mundo virtual.

La realización de estos ilícitos se lleva a cabo a través de redes telemáticas y la interconexión de computadoras. Las ventajas y las necesidades del flujo nacional e internacional de datos conlleva la posibilidad creciente de la comisión de conductas delictivas, por eso puede señalarse que el crimen cibernético constituye un reto considerable

tanto para los legisladores como para las autoridades encargadas de la procuración y administración de justicia.

En el Código Penal del Distrito Federal

Corrupción de personas menores de edad o personas que no tengan capacidad para comprender el significado del hecho

Artículo 183. Al que comercie, distribuya, exponga, haga circular u oferte a menores de dieciocho años de edad o personas que no tengan la capacidad de comprender el significado del hecho o de personas que no tienen capacidad de resistir la conducta, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter lascivo o sexual, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de uno a cinco años de prisión y de quinientos a mil días multa.

Corrupción de menores e incapaces

Artículo 184. Al que por cualquier medio, obligue, procure, induzca o facilite a una persona menor de dieciocho años de edad o personas que no tengan la capacidad de comprender el significado del hecho o de personas que no tienen capacidad de resistir la conducta, a realizar actos de exhibicionismo corporal, lascivos o sexuales, simulados o no, con fin lascivo o sexual, prostitución, ebriedad, consumo de drogas o enervantes, prácticas sexuales o a cometer hechos delictuosos, se le impondrán de siete a doce años de prisión y de mil a dos mil quinientos días multa.

Cuando de la práctica reiterada de los actos de corrupción, la persona menor de dieciocho años de edad o personas que no tengan la capacidad de comprender el significado del hecho o de personas que no tienen capacidad de resistir la conducta, adquiriera los hábitos del alcoholismo, fármaco dependencia, se dedique a la prostitución, práctica de actos sexuales, a formar parte de una asociación delictuosa o de la delincuencia organizada, las penas serán de diez a quince años de prisión y de mil a dos mil quinientos días multa.

Al que procure o facilite la práctica de la mendicidad, se le impondrán de cuatro a nueve años de prisión y de quinientos a mil días multa.

Cuando los actos de corrupción a los que se refiere este artículo se realicen reiteradamente contra menores de dieciocho años de edad o personas que no tengan la capacidad de comprender el significado del hecho o de personas que no tienen capacidad de resistir la conducta, o

éstos incurran en la comisión de algún delito, la prisión se aumentará de tres a seis años.

No constituye corrupción el empleo de los programas preventivos, educativos o informativos que diseñen e impartan las instituciones públicas, privadas o sociales, que tengan por objeto la educación sexual, educación sobre la función reproductiva, prevención de infecciones de transmisión sexual y embarazo de adolescentes.

Pornografía infantil

Artículo 187. Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, audio grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos; se le impondrán de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

Al que fije, imprima, video grabe, audio grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participe una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, se le impondrá la pena de siete a doce años de prisión y de mil a dos mil días multa, así como el decomiso y destrucción de los objetos, instrumentos y productos del delito.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene, distribuya, comercialice, arriende, exponga, publicite, o difunda el material a que se refieren las conductas anteriores.

Al que permita directa o indirectamente el acceso de un menor a espectáculos, obras gráficas o audio visuales de carácter lascivo o sexual, se le impondrá prisión de uno a tres años y de cincuenta a doscientos días multa.

No constituye pornografía el empleo en los programas preventivos, educativos o informativos que diseñen e impartan las instituciones públicas, privadas o sociales, que tengan por objeto la educación

sexual, educación sobre la función reproductiva, prevención de infecciones de transmisión sexual y embarazo de adolescentes.

Artículo 188. Al que almacene, compre, arriende el material a que se refiere el artículo anterior, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa.

Fraude

Artículo 230. Al que por medio del engaño o aprovechando el error en que otro se halle se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

Fraude específico

Artículo 231. Se impondrán las penas previstas en el artículo anterior, a quien:

[...]

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución; o

Aunque los delitos patrimoniales no sufren una modificación en su estructura por la utilización de tecnología en la comisión de los mismos, es necesario que el legislador considere de forma constante esta circunstancia, ya que las formas de llevarlos a cabo cambian constantemente. De la misma manera, las autoridades encargadas de investigar y perseguir el delito deben tener el conocimiento necesario para poder entender que estos delitos se pueden realizar sin siquiera existir una relación o el conocimiento entre los sujetos que intervienen, de hecho cada vez aumentan las formas de realización a través de una computadora o del sistema de Internet, y el sujeto pasivo sufre el detrimento patrimonial sin haberle visto la cara al sujeto que realiza la acción.

Extorsión

Artículo 236. Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de dos a ocho años de prisión y de cien a ochocientos días multa.

Además de las penas señaladas en el primer párrafo, se impondrán de dos a seis años de prisión, cuando en la comisión del delito: [...]

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica.

Esta figura ha sido necesario revisarla detenidamente, ya que representa un serio problema de seguridad nacional, la necesidad de generar un tipo penal autónomo, ya que desde mi particular punto de vista existe una afectación en el sujeto pasivo con independencia de causarle un detrimento patrimonial: la llamada telefónica misma causa una afectación en el ánimo del sujeto pasivo, generando un miedo que resulta difícil reparar. México ha sufrido un aumento considerable de este delito, y es necesario que exista un registro nacional de usuarios de teléfonos celulares para evitar que eso suceda. Es obligación de los concesionarios proporcionar los datos y restringir el uso de los mismos desde centros penitenciarios, que es, la mayoría de las veces, desde donde se realizan las mismas.

Delincuencia organizada

Artículo 254.- Cuando tres o más personas se organicen o acuerden organizarse de forma permanente o reiterada para cometer alguno o algunos de los delitos siguientes, se les impondrán de cuatro a diez años de prisión y de doscientos hasta mil días multa, sin perjuicio de las penas que correspondan por el delito o delitos que se cometan:

- I. Ataques a la paz pública; de conformidad con lo establecido por el artículo 362 de este Código;
- II. Corrupción de persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta establecidos en los artículos 184, 185 primero, segundo, tercero, cuarto y quinto párrafos y 186 en sus fracciones I y II de este Código;
- III. Extorsión, conforme al contenido del primer párrafo del artículo 236 de este Código;
- IV. Falsificación de documentos públicos, de acuerdo con el primer párrafo del artículo 339 de este Código;
- V. Homicidio, de conformidad con el artículo 128 de este Código;
- VI. Lenocinio, previsto en los artículos 189 y 189 bis de este Código;
- VII. Operaciones con recursos de procedencia ilícita, de conformidad con el párrafo primero del artículo 250 de este Código;
- VIII. Pornografía, establecido en los artículos 187 y 188 de este Código;

- IX. Privación de la libertad personal, en concordancia con lo previsto por los artículos 160 y 161 de este Código;
- X. Retención y sustracción de menores e incapaces, de conformidad con el artículo 171 de este Código;
- XI. Robo de conformidad con el artículo 224, fracciones II y VIII, en su hipótesis primera;
- XII. Secuestro, previsto en el artículo 163 y 163 Bis de este Código;
- XIII. Tráfico de menores, contemplado en el párrafo tercero del artículo 169 de este Código;
- XV. Turismo sexual, establecido en el artículo 186 de este Código;
- XVI. Trata de personas, establecido en el artículo 188 bis de este Código; y
- XVII. Explotación laboral de menores o personas con discapacidad física o mental, previsto en los artículos 190 bis y 190 ter de este Código.

A quien tenga funciones de administración, dirección o supervisión en la delincuencia organizada, se le impondrán de seis a doce años de prisión y de cuatrocientos a dos mil días multa, sin perjuicio de las reglas de concurso para la imposición de sanciones.

La criminalidad organizada

La criminalidad organizada ha venido presentando, en los últimos años, un extraordinario incremento de sus actividades, afectando a toda la comunidad internacional y abarcando una gran cantidad de sectores de la actividad económica y social, esto derivado de los procesos de globalización, siendo determinante la aceleración en los medios de comunicación y transporte.¹⁴⁴ Del mismo modo, algunos de estos grupos dedicados a la criminalidad organizada tienen diversas conexiones con otros grupos similares en otros países. El crimen organizado debe ser distinguido de cualquier otro tipo de manifestaciones de criminalidad, ya que, como se ha mencionado, sus actividades son identificadas como las de una corporación con una permanencia y finalidad común, lo que le da características particulares del resto de los grupos criminales.¹⁴⁵

Descubrimientos recientes sugieren que los grupos del crimen organizado han obtenido en los últimos tiempos material y tecnología de

punta, lo que los sitúa en una posición estratégica para sus actividades. Este material y tecnología es obtenido gracias a la ayuda de grupos terroristas, lo que representa una amenaza para la paz, seguridad y relaciones internacionales.¹⁴⁶ A modo de ejemplo, un estudio realizado en Estados Unidos de América ha podido comprobar la increíble proliferación de delincuentes y de grupos dedicados al crimen organizado en ciudades de ese país. Se calcula que entre 1961 y 1970 hubo un incremento de 74% en el número de grupos criminales en distintas ciudades, pero ha sido aún mayor de 1980 a 1992, ya que se calcula un aumento de 345%. En 1996 se calculó que aproximadamente el 57% de todas las ciudades de más de 200,000 personas en Estados Unidos presentaban un problema serio de delincuencia organizada.¹⁴⁷ Dicho esto, es necesario que se examine la legislación nacional de los Estados, para hacer más viable la cooperación entre los mismos, a efecto de conformar un grupo multinacional de lucha frontal contra el crimen organizado.

A este respecto, los mayores prototipos de grupos dedicados al crimen organizado transnacional son: la mafia siciliana (cuya ramificación más conocida y una de las más violentas está en los Estados Unidos de Norteamérica, la Cosa Nostra); la mafia japonesa, llamada Yakuza; los cárteles de la droga de la mafia colombiana, principalmente el Cártel de Cali y el Cártel de Medellín; los "Señores de la Droga" del Triángulo Dorado de Burma, Tailandia y Laos; y las triadas chinas.¹⁴⁸ Las actividades llevadas a cabo por los diversos grupos del crimen organizado requieren de un significativo grado de cooperación y organización para proveerse de manera ilícita de los bienes que requieren para sus actividades. Como cualquier otro negocio, el negocio del crimen requiere una especialización considerable y una amplia capacidad de coordinación. A esto debe añadirse la utilización de la violencia y la corrupción como medios para conseguir sus fines. Algunos de estos grupos se encuentran altamente especializados con respecto a alguna forma particular de actividad criminal, como sería

¹⁴⁴ Delgado Marín, J. La criminalidad organizada. Editorial J.M. Bosch, Barcelona, 2001. p. 22.

¹⁴⁵ Cherif Bassiouni, M. y Vetere, E. "Towards Understanding Organized Crime and its Transnational Manifestations" en *Organized Crime, A compilation of United Nations Documents 1975-1998*. Transnational Publishers, Inc., 1998, p. XXVI.

¹⁴⁶ United Nations, Economic and Social Council; Commission on Crime Prevention and Criminal Justice, Status of the Preparations for the World Ministerial Conference on Organized Transnational Crime: Report of the Secretary-General, U.N. Doc. E/CN.15/1994/4 (25 February 1994). A compilation of United Nations Documents 1975-1998. Transnational Publishers, Inc., 1998, p. 594.

¹⁴⁷ Thornberry, T. P., AAVV, *Gangs and Delinquency in Developmental Perspective*. Cambridge University Press, New York, 2003, p. 2.

¹⁴⁸ Es casi seguro que existan en otros grupos criminales, pero los señalados en este párrafo son los que se consideran como los más conocidos y violentos dentro del crimen organizado internacional, según el criterio de las Naciones Unidas.

la prostitución o el tráfico de drogas; otros por el contrario tienen un margen más amplio para el desarrollo de sus actividades criminales, como sería la falsificación y el uso de tarjetas de crédito, y diversos tipos de fraude financiero.

Conclusiones

Haciendo un análisis concreto, es importante señalar que se debe de actuar de la manera más eficaz y con los medios tecnológicos disponibles para evitar este tipo de delitos y que no se sigan cometiendo con tanta impunidad. Se debe legislar de una manera seria y honesta, procurando homologar criterios y recurriendo a las personalidades de reconocimiento internacional que tienen el conocimiento, tanto técnico como legal, para regular estas figuras.

Debido a la naturaleza virtual de los delitos informáticos puede volverse confusa la tipificación de éstos ya que, a nivel general, se poseen pocos conocimientos y experiencias en el manejo de esta área. Desde el punto de vista legislativo es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.

Nuevas formas de hacer negocios, como el comercio electrónico, pueden no encontrar el eco esperado en los individuos y en las empresas hacia los que va dirigido debido a este tipo de delitos, por lo que se deben crear instrumentos legales internacionales efectivos que ataquen esta problemática, con el único fin de tener un marco legal único que se utilice como soporte para el manejo de este tipo de transacciones. Con el avance de la tecnología y las comunicaciones la información que posee la gente, sea cual sea la misma, se archiva en su mayoría en sistemas o medios electrónicos. Aunque existe la posibilidad de codificar la información que se encuentra contenida en éstos, es una realidad que la mayoría de la gente no lo hace.

Un medio informático es aquel que utiliza procesos de información automatizada, sin embargo un medio electrónico es cualquier bien que utilice electricidad, por lo mismo éste es el género de aquél.

La denominación "delitos informáticos" es poco atinada, ya que muchas de las conductas que se tutelan en los mismos pueden ser realizadas por mecanismos no informáticos, por eso, se debe de cambiar la denominación al género y no a la especie, para llamarse "delitos cometidos por medios electrónicos". De esta forma se obtendrían tipos genéricos que no quedarían rezagados por el avance de la tecnología a corto plazo.

No existe un consenso sobre la definición de los mal llamados delitos informáticos (delitos cometidos por medios electrónicos), por lo anterior proponemos definirlos como toda conducta autónoma, en la cual intervienen medios electrónicos que alteren o destruyan la seguridad de la información (seguridad informática) contenida en cualquier medio electrónico.

En los delitos cometidos por medios electrónicos el sujeto activo puede o no tener conocimientos sobre medios electrónicos; sin embargo, en los cometidos a través de Internet los sujetos activos generalmente tienen conocimientos técnicos o profesionales superiores a los del usuario promedio.

Dada la continua evolución de Internet y los medios electrónicos resulta imposible delimitar todas las conductas delictivas que se pueden crear, por lo cual hay que crear tipos penales genéricos que puedan englobar la mayoría de las conductas.

Todos los tipos penales contienen bienes jurídicos tutelados y, en los delitos cometidos por medios electrónicos, el bien jurídico tutelado es la seguridad informática, entendiendo que no se protege directamente a la información, sino que la información esté segura y no pueda ser violentada por un agente externo o diverso a su autor, sea cual fuere el contenido de la misma.

Bibliografía

- ALONSO PÉREZ, F., Delitos contra el patrimonio y contra el orden socioeconómico. Aspectos penales y criminológicos, Editorial Colex, Madrid, 2003.
- Arilla Bas, F. El procedimiento penal en México, Ed. Porrúa, México, 1997.
- Bramont-Arias, Luis Alberto. Código Penal Anotado. Ed., Lima, 1998.
- CALDERÓN CEREZO, A., CHOCLAN MANTALVO, J.A., Derecho Penal., Parte Especial, Tomo II Editorial Bosch, Barcelona, 2001.
- CAMACHO LOSA, L., El delito informático, Gráficas Cóndor, Madrid, 1987.
- Cherif Bassiouni, M. y Vetere, E. "Towards Understanding Organized Crime and its Transnational Manifestations" en Organized Crime, A compilation of United Nations Documents 1975-1998. Transnational Publishers, Inc., 1998, p. XXVI.
- Colín Sánchez, G. Derecho mexicano de procedimientos penales, Ed. Porrúa, , México, 1979.
- CORCOY BIDASOLO, M. Y JOSHI JUBERT, U., "Delitos contra el patrimonio cometidos por medios informáticos", Revista Jurídica de Cataluña, Núm. III, Barcelona, 1988.
- CORCOY BIDASOLO, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", en MIR PUIG, S., (comp.), Delincuencia informática, Editorial PPU, Barcelona, 1992.

- CHOCLAN MONTALVO, J. A., "Fraude informático y estafa por computación", en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001.
- DAVARA RODRÍGUEZ, M.A., Manual de derecho informático, Editorial Aranzadi, Pamplona, 1997.
- DE ALFONSO LASO, D., "El hackerin blanco. Una conducta ¿punible o impune?", en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001.
- De Miguel Asencio, P., Derecho privado de Internet. Editorial Civitas, Madrid, 2000.
- Delgado Marín, J. La criminalidad organizada. Editorial J.M. Bosch, Barcelona, 2001.
- GONZALEZ RUS J. J., "Aproximaciones al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos," Revista de la Facultad de Derecho de la Universidad Complutense, Núm. 12, Madrid, 1986.
- _____, "Delitos contra el patrimonio y contra el orden socioeconómico (I)", en Compendio de derecho penal español. Parte Especial, COBO DEL ROSAL, M. (dir.), Editorial Marcial Pons, Madrid, 2000.
- Gutiérrez Francés, M. "Notas sobre la delincuencia informática: atentados contra la 'información' como valor económico de empresa" en: Mazuelos Coello, J. (comp.). Derecho Penal Económico y de la Empresa. Ed. San Marcos, Lima, 1997.
- IJENA LEIVA, R. J., Chile, la protección penal de la intimidad y el delito informático, Editorial Jurídica de Chile, Santiago.
- MARCHENA GÓMEZ, M., "El sabotaje informático: entre los delitos de daños y desórdenes públicos", en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001.
- MATA Y MARTÍN, R. M., Delincuencia informática y derecho penal, Editorial Edisofer, Madrid, 2001.
- Matellanes Rodríguez, N. Algunas notas sobre las formas de delincuencia informática en el Código penal. Hacia un Derecho Penal sin fronteras. Colex, Madrid, 2000..

- Mazuelos Coello, J., "Protección jurídico penal de la información como valor económico de la empresa", en Revista Legal del Estudio Muñiz, Forsyth, Ramírez, Pérez-Taimán y Luna-Victoria Abogados, marzo de 1999.
- MORANT VIDAL, J., Protección penal de la intimidad frente a las nuevas tecnologías, Editorial Práctica de Derecho, Valencia, 2003.
- MORON LERMA, E., Internet y derecho penal: hacking y otras conductas ilícitas en la Red, Editorial Aranzadi, Navarra, 2002.
- MUÑOZ CONDE, F., Derecho penal. Parte especial, Editorial Tirant lo Blanch, Valencia, 2002.
- Orellano Wiarco, O. Teoría del delito - Sistemas Causalista y Finalista, Ed. Porrúa, México, 1995.
- ORTS BERENGUER, E. Y ROIG TORRES, M., Delitos informáticos y delitos comunes cometidos a través de la informática, Editorial Tirant lo Blanch, (Col. Los Delitos), Valencia, 2001.
- ROMEO CASABONA, C.M., Poder informático y seguridad jurídica, Editorial Fundesco, Madrid, 1987.
- ROVIRA DEL CANTO, E., Delincuencia informática y fraudes informáticos, Editorial Comares, Granada, 2002.
- RUÍZ MARCO, F., Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática, Editorial Colex, Madrid, 2001.
- RUIZ VADILLO, E. Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad informática, Poder Judicial, Núm. Especial IX, Madrid, 1989.
- SIEBER, U., "Documentación para una Aproximación al Delito Informático", en MIR PUIG, S., (comp.), Delincuencia Informática, Editorial PPU, Barcelona, 1992.
- _____, "Criminalidad informática: peligro y prevención", en MIR PUIG, S., (comp.), Delincuencia informática, Editorial PPU, Barcelona, 1992.
- Silva Sánchez J. M., Aproximación al Derecho Penal Contemporáneo. Bosch Editores, Barcelona, 1992, p. 69.
- SNEYERS, A., El fraude y otros delitos informáticos, T.G.P., Madrid, 1990.

- TÉLLEZ VALDÉS, J., Derecho informático, Ed. Mc Graw Hill, México, 1996.
- Thornberry, T. P., et. al., Gangs and Delinquency in Developmental Perspective. Cambridge University Press, New York, 2003, p. 2.
- United Nations, Economic and Social Council; Commission on Crime Prevention and Criminal Justice, Status of the Preparations for the World Ministerial Conference on Organized Transnational Crime: Report of the Secretary-General, U.N. Doc. E/CN.15/1994/4 (25 February 1994). A compilation of United Nations Documents 1975-1998. Transnational Publishers, Inc., 1998, p. 594.
- VIVES ANTÓN, T.S., y GONZALEZ CUSSAC, J.L., Comentarios al Código Penal de 1995, Editorial Tirant lo Blanch, Valencia, 1996.
- _____, y _____, Derecho penal. Parte especial, Editorial Tirant lo Blanch, Valencia 1999.

Índice

Introducción	XI
CAPÍTULO I	
El internet	1
1.1 Historia de Internet	2
1.2 Las "autoridades" en Internet	7
1.3 El funcionamiento de Internet	8
1.4 Concepto de información	11
1.5 Concepto de delito informático	13
CAPÍTULO II	
Delitos cometidos en internet	21
2.1 Delitos contra el hardware	21
2.2 Delitos contra el software	21
2.3 Delitos contra la memoria del ordenador	22
CAPÍTULO III	
Conductas ilícitas cometidas en internet	23
CAPÍTULO IV	
Sujeto activo	27
4.1 Hackers	30
4.2 Crackers	32

4.3 Cyberpunk	34
4.4 Phreaker	35
CAPÍTULO V	
Sujeto pasivo	39
CAPÍTULO VI	
Las amenazas de internet a la información	41
CAPÍTULO VII	
La criminalidad informática	45
CAPÍTULO VIII	
Nociones generales del delito.....	49
CAPÍTULO IX	
El delito informático	49
9.1 Delitos contra el patrimonio	51
CAPÍTULO X	
Clasificaciones	55
CAPÍTULO XI	
Modalidades	61
11.1 Intrusismo informático o hacking informático	61
11.2 Hurto de tiempo informático.....	65
11.3 Espionaje informático	67
11.4 Piratería informática	68
11.5 Sabotaje informático.....	69
11.6 Fraude informático.....	72
CAPÍTULO XII	
Delitos informáticos en el código penal español	75
12.1 Delitos contra la libertad: amenazas y coacciones.....	75
12.2 Delitos contra la libertad sexual.....	76
12.3 Delitos contra la intimidad: descubrimiento y revelación de secretos	76
12.4 Delitos contra el honor: calumnia e injuria.....	80
12.6 Virus informáticos.....	84

CAPÍTULO XIII	
Delitos informáticos en la legislación mexicana.....	75
13.1 Legislación en materia penal en México	87
13.2 La acción penal en México	89
13.3 Los delitos informáticos en la legislación mexicana	90
Conclusiones.....	105



Delitos informáticos y Derecho penal
Luis Azaola Calderón
se terminó de imprimir en Enero de 2010
en los talleres de Diseño e Impresos Sandoval
Tel.: 5793-4152, 5793-7224
la edición consta de 1000 ejemplares
más sobrantes para reposición.