Revista de Derecho y Ciencia Política, Vol. 59 (N° 2). Lima, 2002. pp. 383 - 410

DELITOS INFORMÁTICOS

Silfredo Hugo Vizcardo
Profesor en la Facultad de Derecho de la UNMSM.

SUMARIO:

1.- Concepto

Producto de la evolución del ingenio humano y de la ciencia, que siempre está a la vanguardia de la creación de mejores posibilidades de vida y sustento, modernamente aparecieron las denominadas «computadoras» u «ordenadores», que revolucionaron el modo de vida social de toda la humanidad, dando origen a la informática, que es concebida como la ciencia de la elaboración, memorización, conservación y análisis y recuperación de datos en forma significativa o

simbólica (Rivera LLanos, pág. 167). Técnicamente concebido, el computador u ordenador es un dispositivo electrónico digital de programa almacenado capaz de memorizar, elaborar o recuperar información o datos.

Se trata de una herramienta muy técnica y sofisticada, de enorme aplicación práctica. Es la única máquina programable, ya que sale de fábrica con una capacidad instalada que constituye su sistema general (posee "capacidad" para interpretar cierto tipo de lenguaje o programa), correspondiendo posteriormente al ingenio del hombre determinar la vastedad de su aplicación objetiva, mediante la inserción de una serie de datos o instrucciones que constituyen los programas de computación. En tal sentido, «las posibilidades del ordenador son inmensas, infinitas; permiten una verdadera enseñanza conforme a las ideas, las necesidades y lo que pretende el hombre, llegando a hacer muchas cosas como éste, pero a mucha velocidad y sin cansancio» (Núñez Ponce, 1996, pág. 19).

Las aplicaciones de las computadoras son diversas dependiendo de los programas que se utilicen. Inciden decisivamente en los diversos niveles de las relaciones humanas. Se constituye en una forma de «inteligencia artificial» de uso instantáneo, práctico y seguro. Pueden utilizarse en los negocios, industria, empresa, medicina, derecho, contabilidad, etc.; puede ser utilizado, como de hecho lo es, tanto por el sector público como el privado.

Actualmente, dentro de la denominada era de la automatización o revolución cibernética (comparable sólo con la revolución industrial), que caracteriza al mundo contemporáneo desde la década de los años 50, no existe un solo sector de la sociedad que no se vea influenciado por la evolución alcanzada por la informática. Una de las principales causas de este fenómeno es el empleo generalizado y globalizado de la internet, concebido como un sistema transnacional de comunicación que, gracias a unos estándares comunes y usando tecnologías y redes de telecomunicación, permite el intercambio y la obtención de información mediante el uso de diversas modalidades de comunicación en línea (listas de correo, grupos de discusión de Usenet, FTP, w w w, chats, etc.).

La utilización de computadoras, es decir, de sistemas informáticos incide fundamentalmente sobre el desarrollo social de cada país (ello en relación directa con el grado de desarrollo cultural y económico) (por ello se dice contemporáneamente que la lucha por el poder político y económico se trasladado del ámbito del control de las grandes energías al del dominio de la información). Esta realidad ha determinado, como contrapartida negativa, la apari-

ción de actos vulnerantes o lesionantes contra los derechos que alrededor de la propiedad o utilización de los medios informáticos se han ido generando y que han fundamentado una nueva gama de bienes jurídicos a proteger. Aparece así la criminalidad por computadora o «delito informático» ("computer crime"), que es definido como «la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software (Miguel Dávara, 1993, pág. 318). Conforme lo señala Tiedemann, con la expresión «criminalidad mediante computadoras» se alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos» (1985, pág. 122).

Se trata de delitos instrumentados mediante el uso del computador. La Organización para la Cooperación económica y el desarrollo, ha definido al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos y/o la transmisión de datos.

Para Camacho, el delito informático es toda acción dolosa que provoca un perjuicio a persona o entidades, sin que necesariamente conlleve un beneficio material para su autor o que, por el contrario produce un beneficio ilícito a su autor aún cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión interviene necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas. Por su parte, Rafael Fernández Calvo define al delito informático como "la realización de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española.

Al respecto, es preciso tener en cuenta lo manifestado por Dávara, en el sentido de que generalmente concurren determinadas características comunes a todas las conductas catalogadas como delitos informáticos, que nos permiten clasificarlas de acuerdo con la función y actividad que se realiza para cometerlos. Estos delitos poseen unas especialidades que les hacen, en ocasiones más difíciles de detectar y, en otras, aún detectados, no son denunciados por múltiples razones, y aun siendo denunciados son difíciles de perseguir. Todos ellos centran su principal actividad en el acceso y/o la manipulación de datos -que se encuentran en soportes informáticos- o de programas de ordenador utilizados en su procesamiento (ob., cit., pág. 322).

Debido a su gran vastedad y especialidad, la tarea de tipificación de esta clase de delitos resulta una labor muy complicada, siendo necesario delimitar con mucha precisión las características adecuadas de la criminalización de estas conductas, y por sobre todo, el bien jurídico afectado, como base de la sistematización. Adicionalmente a ello, indica Núñez, debe encuadrarse la problemática de la prueba de la comisión de los delitos informáticos, con su descubrimiento y comprobación mediante la Auditoria Informática (ob. cit. pág. 253).

En tal sentido, podemos apreciar que contemporáneamente el uso de las computadoras y su interconexión, ha dado lugar a un fenómeno de nuevas dimensiones: el delito instrumentado mediante el uso del computador (denominado "delito informático", "delito electrónico", "delito relacionado con las computadoras", "crímenes por computadora" o "delincuencia relacionada con el ordenador". Si bien no existe aún una medida exacta de la importancia de estas transgresiones, es probable que su incidencia se acentúe con la expansión del uso de computadoras y redes telemáticas. Los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas, tal como la interferencia en una red bancaria para obtener, mediante una orden electrónica, un libramiento ilegal de fondos o la destrucción de datos. el tema plantea, además, complejos perfiles para el derecho internacional cuando el delito afecta a más de una jurisdicción nacional (Carlos Correa y otros, 1987, pág. 295).

Por ello bien dice Tiedemann que la tarea del derecho no es la de quedarse atado a viejas categorías teóricas que nada sirven sino más bien de adaptarse y proveerse de nuevas formas de prevención y protección a la sociedad. Es por ello que el Derecho penal debe revisarse así mismo, y encuadrarse en estas situaciones que protejan a las personas y no esconderse en lagunas legales que no ayudan a nadie.

El Derecho penal debe también prevenir la comisión de éste tipo de hechos que de ninguna manera pueden ser entendidos como errores involuntarios ya que son realizados por personas que generalmente están familiarizadas y se encuentran especializadas en el trabajo con computadoras y que fácilmente pueden conocer como entrar en los archivos de datos de cualquier individuo.

El Derecho penal debe resguardar los intereses de la sociedad, evitando manipulaciones computarizadas habituales o no, basadas en conocimiento de los objetos, programas, así como de algunas informaciones que extiendan y hagan imposible la detección de estos ilícitos (El desarrollo actual y moderno

nos ha traído avances importantes para la humanidad, pero es penoso a su vez que vengan acompañados de hechos delictivos no deseados).

2.- Tipificación y Clasificación

Conforme a la definición genérica de la Organización para la Cooperación Económica y el Desarrollo, delito informático («computer crime») es «cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos». Estos delitos, conforme a Sieber, pueden ser clasificados en las siguientes categorías:

a) Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;
b) Espionaje informático y robo de software;
c) Sabotaje informático;
d) Robo de servicios;
e) Acceso no autorizado a sistemas de procesamiento de datos; y,
f) Ofensas tradicionales en los negocios asistidos por computador.

Por otro lado (en su clasificación), los tipos de delitos informáticos reconocidos por Naciones Unidas son:

1) Fraudes cometidos mediante manipulación de computadoras:

a) Manipulación de los datos de entrada.- Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales del procesamiento de datos en la fase de adquisición de los mismos.

b) Manipulación de programas.- Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el agente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático, para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) Manipulación de los datos de salida.- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el

fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) **Manipulación informática.-** Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica salami" o "técnica del salchichón", en la que "rodajas muy finas", apenas perceptibles de transacciones financieras, se van sacando repetida y automáticamente de una cuenta y se transfieren a otra.

2) Falsificaciones informáticas:

a) **Como objeto.-** Cuando se alteran datos de los documentos almacenados en forma computarizada.

b) **Como instrumento.-** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3) Daños o modificaciones de programas o datos computarizados:

a) **Sabotaje informático.-** Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: "virus", "gusanos" o "bomba lógica o cronológica".

b) **Acceso no autorizado a servicios y sistemas informáticos.-** Ello por diversos motivos; desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones recurriendo a diversos medios. El delincuente puede aprovechar la falta de rigor de las medidas de se-

guridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c) **Reproducción no autorizada de programas.-** Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Los delitos informáticos también pueden ser clasificados en atención a los siguientes criterios:

a) **Como instrumento o medio.-** Comprendiendo a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito. Ejemplo: Los falsificadores de tarjetas de crédito, billetes y/o documentación oficial (debiendo agregar a los equipos que emiten hologramas oficiales de verificación y de tenencias).

b) **Como fin u objeto.-** En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Para ejemplificar este criterio que más sino mencionar tanto a los crackers como a los hackers, quienes han revolucionado a los programas de seguridad y se han convertido en un filtro más en la efectividad del desarrollo de software especializado.

Con respecto al tema, el derecho comparado informa la necesidad actual de combatir esta especial forma delictual, con medidas jurídico penales especializadas que trasciendan los moldes tradicionales del derecho punitivo, que permitan la necesaria adopción de medidas legislativas precisas y oportunas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las formas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentar tal problemática.

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda

Ley contra la Criminalidad Económica del 15 de mayo de 1986, en la que se contemplan los siguientes delitos:

- Espionaje de datos (202 a).
- Estafa informática (263 a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos; inclusive la tentativa es punible.
- Sabotaje informático (303 b), destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266 b).

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los países escandinavos y en Austria.

El legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, observan los especialistas, no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática, el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional, a comportamien-

tos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión, que pasan por la utilización abusiva de instalaciones informáticas. Las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos.

En Austria, la Ley de reforma del Código Penal de 22 de diciembre de 1987, contempla los siguientes delitos: Destrucción de datos (personales, no personales y los programas), estafa informática (causar perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automáticos a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos). Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

En Francia, la Ley número 88-19 de 5 de enero de 1988, regula el fraude informático, tipificando las conductas de: Acceso fraudulento a un sistema de elaboración de datos (se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema), sabotaje informático (impedir o falsear el funcionamiento de un sistema de tratamiento automático de datos), destrucción de datos (introducir, intencionalmente y con menosprecio de los derechos de los demás, datos en un sistema de tratamiento automático de datos o suprimir o modificar los datos que este contiene o los modos de tratamiento o de transmisión), falsificación de documentos informatizados y uso de documentos informatizados falsos.

En Estados Unidos es importante mencionar la adopción en 1994, del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986 (con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etc. y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus).

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan un daño por la transmisión del virus, el castigo de hasta diez años en prisión federal más una multa, y para aquellos que lo transmiten sólo de manera imprudencial, la sanción fluctúa entre una multa y un año en prisión. La referida Acta de 1994 precisa también que el creador de un virus no podrá escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad, en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad, que constituyen el objetivo principal de esta Ley.

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal, relativas a los delitos informáticos en las que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etc. El objetivo de los legisladores al realizar esta enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la inter-

ferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y a las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos, así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el Estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos, sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

En Gran Bretaña debido a un caso de hacking en 1991, comenzó a regir la Cómputer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que estos causen.

En los países latinoamericanos no existe una legislación específica al respecto. En Argentina no encontramos la tipificación de los delitos informáticos, sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la ley 11.723 de propiedad intelectual, gracias al decreto número 165/94 del 8 de febrero de 1994.

Por su parte, en Chile (que fue el primer país latinoamericano en sancionar una ley contra delitos informáticos <7 de junio de 1993>), se prevé que cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización, intercepta, interfiere, recibe, usa, altera, daña o destruye una computado-

ra, un sistema o red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o red».

Como puede apreciarse, la problemática de los delitos informáticos requiere un estudio especial y conocimiento técnico científico, para poder cumplir con la labor de tipificar suficientemente estos delitos con vista a una adecuada protección social, ya que es creciente la expansión de la cultura informática en nuestro medio, tanto en el sector público como en el privado (el comercio, la actividad bancaria, la actividad industrial, el negocio de los particulares y empresas, etc.). Es necesario prepararse para prevenir y reprimir este tipo de conductas, ya que de acuerdo al axioma de la «auditoria», todo ilícito que tenga la más mínima posibilidad de ocurrir, ocurrirá inexorablemente si no se lo previene (también es preciso tener en cuenta que es importante la influencia de las posibilidades técnicas de nuevas y mas avanzadas máquinas, programas, capacidad de archivos de datos, etc.)

Todo ello nos permite decir que siendo tan amplio el espectro delictivo informático y para evitar la distorsión y dispersidad de normas, sería conveniente postular un nuevo Título en el Libro Segundo del Código Penal, que trate la tipificación coherente y sistemática, de todas las conductas criminales que esta actividad involucra. Esto en razón de que ha llegado ya el momento que el Derecho penal rompa su moldura rígida clásica y evoluciones conjuntamente con el desarrollo del conocimiento científico, permitiendo así la real protección de la seguridad y protección de la sociedad, ya que al parecer, se está quedando anticuado en este aspecto de los delitos informáticos.

En nuestro sistema penal, que no tiene suficientemente desarrollado el tema, los delitos informáticos tienen su radio de acción principalmente en los atentados contra los derechos de autor, violación de la intimidad personal, falsificación de documentos informáticos, entre otros. En el campo de los delitos patrimoniales, podemos apreciar que nuestro texto punitivo tipifica ciertas conductas posibles de ser cometidas mediante medios informáticos, tales como el hurto agravado utilizando sistema de transferencia electrónica de fondos de la telemática en general, descrito en el numeral 3 del segundo párrafo del artículo 186; el delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (Inciso 8 del artículo 198), e incluso el delito de daños (Art. 205) desde la perspectiva del atentado contra el hardware (en su condición de bien material).

3.- Modalidades Delictivas

Siguiendo esta técnica legislativa, y en atención a los vacíos legales existentes en esta materia tan especializada, es que mediante la disposición introducida por ley 27309 del 17 de julio del 2000, se modifica el Título V, del Libro Segundo del C. P., insertando un nuevo capítulo (Capítulo X), denominado "Delitos Informáticos", que, como hemos visto, sólo constituyen un sector parcial de este género delictivo, orientado específicamente al ámbito patrimonial.

Por la similitud del texto patrio, consideramos que la fuente directa la encontramos en el proyecto de «ley de informática» del Ministerio de Justicia de Chile (abril de 1986), que establece que: «cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o red».

El Título contiene la siguiente clasificación típica:

a.- Intrusismo informático.....(primera parte).....Art. 207-A
b.- Fraude informático.....(segunda parte)....Art. 207-A
c.- Sabotaje informático.....Art. 207-B
d.- Circunstancias agravantes.....Art. 207-C

4.- Intrusismo Informático

4.1.- Presentación de la Norma

Artículo 207-A: El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidos a ciento cuatro jornadas.

Si el agente actúo con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

4.2.- Bien Jurídico protegido

Por su misma ubicación legislativa, el tipo en comentario defiende el bien jurídico «patrimonio», desde la perspectiva del derecho a la propiedad que tiene el sujeto pasivo a su base de datos, sistema o red de computadoras.

Se trata de un delito pluriofensivo, ya que atenta no sólo contra el patrimonio, sino también contra el orden económico, el sistema informático, la libertad e intimidad personal y la titularidad del derecho intelectual.

4.3.- Tipo objetivo de lo injusto

4.3.1.- Acción Delictiva

Se trata de un tipo de mera actividad, en el que para su consumación resulta suficiente que el sujeto haya ingresado o utilizado indebidamente la base de datos o sistema de computadoras, sin necesidad de un resultado material separable de la conducta.

Se señala también como característica del tipo, el de ser uno de peligro, que en general no exige el resultado dañoso, por lo que la consumación se produce cuando el agente despliega la conducta que provoca la puesta en peligro o el riesgo del bien jurídico, que en el tipo en estudio está representado por la referencia al intrusismo del sujeto activo que utiliza o ingresa al sistema "para" diseñar, ejecutar, etc.

La actividad de acceso a un sistema informático sin autorización se conoce como "HACKING". Desde la perspectiva doctrinaria, encontramos aquí como de posible realización, actos de espionaje informático, manipulación de datos de entrada y programas, acceso no autorizado a sistemas de procesamiento de datos, robo de software, etc.

Evidentemente, por tratarse de bienes de libre disposición, el consentimiento aparece en este delito como causa de atipicidad. Asimismo, siendo posible la revocatoria, ésta no ha de ser entendida en términos absolutos, ya que dependerá en cada caso de las circunstancias propias

del titular del derecho, quien en definitiva determinará los alcances y duración de su autorización. Evidentemente no cabe entender la revocatoria con alcances retroactivos.

Por otro lado, resulta interesante apreciar lo esbozado por Juan Blossiers y Sylvia Calderón, con respecto a las características de estos delitos (ob. cit. pág. 34):

a) **Acumulación de la información.-** La tendencia generalizada de centralizar y consolidar la información corporativa en grandes bases de datos, sobre la cual interactúan numerosos usuarios, posibilita considerablemente el acceso a cualquier tipo de información, una vez que se han violado las medidas de seguridad o control de acceso.
b) **Inexistencia de Registros Visibles.-** La información grabada se registra en impulsos eléctricos sobre soportes magnéticos que son ilegibles para el ojo humano. Con lo cual la posibilidad de descubrir un hecho delictivo por simple inspección ocular resulta nula e imposible.
c) **Falta de evidencias en la Alteración de Datos y Programas.-** La alteración de programas y datos pregrabados en soportes magnéticos pueden hacerse sin dejar rastro alguno, ya que no existirán indicios del ingreso de un extraño al sistema.
d) **Eliminación de pruebas.-** Es sumamente fácil en caso de ser descubierto, desaparecer programas manipulados o ficheros completos de datos alterados desde el teclado de una computadora tan sólo pulsando una tecla o enviando una instrucción de borrado lo cual puede posteriormente reportarse como error fortuito.
e) **Especialidad del Entorno Técnico.-** Incluso los sistemas más sencillos presentan gran complejidad en términos de la capacidad técnica y en el tiempo necesario para entender en detalle lo que realiza el sistema y de la forma como lo ejecuta. Generalmente y después de corto tiempo los usuarios comienzan a aceptar la integridad del sistema sin cuestionárselo, sobre todo si ha sido diseñado para que la intervención humana sea cada vez de mínima incidencia.
f) **Dificultad para proteger Ficheros o Archivos.-** La protección de la información almacenada en soportes magnéticos es muy compleja.
g) **Concentración de funciones.-** La separación de funciones incompatibles generalmente no existen en los centros de procesos de datos, especialmente en los de dimensiones mediana y pequeña en los que predominan los conceptos de funcionalidad y versatilidad del personal sobre la seguridad.

h) **Falta de Controles Internos de Seguridad.-** La inexistencia del desarrollo de programas de software de medidas de control interno y pistas de auditoría en las nuevas aplicaciones posibilita las manipulaciones fraudulentas.

i) **Carencia de Controles del Personal Técnico.-** La mayoría de los controles establecidos para la aplicación de los ficheros pueden ser fácilmente burlados por técnicos informáticos con cierta calificación.

j) **Dispersión Territorial de los Puntos de Entrada al Sistema.-** La mayoría de los sistemas informáticos están diseñados sobre el concepto de una marcada descentralización de la información que permita acceder a la información de manera cómoda desde donde está el usuario o donde se producen los datos de entrada, y justamente mientras se establecen medidas de control centralizados estas suelen ser inexistentes en la práctica pues los puntos remotos de entrada permiten el acceso al sistema.

k) **Interdependencia de Redes de Transmisión.-** Los sistemas informáticos generalmente se basan en una red de comunicaciones para su funcionamiento y se prevé que la tendencia es que la totalidad de las comunicaciones se harán por las redes públicas que son compartidas por múltiples usuarios y que adicionalmente no es posible establecer medidas de control sobre ellas.

4.3.2.- Objeto material de la acción

La acción material del sujeto activo no recae sobre el aspecto extrínseco del ordenador o computador, denominado hardware (que como aparato físico, ya se encuentra protegido en otras figuras delictivas: hurto, robo, apropiación ilícita, daños, etc.), sino sobre su aspecto intrínseco, que contiene su sistema de soporte lógico, identificado con el concepto del software (que es el conjunto de instrucciones o expresiones que tienen como finalidad dotar al ordenador o computador de la capacidad de actuación determinando sus posibilidades de uso y aplicaciones concretas (Núñez, ob., cit., pág. 28).

La acción también recae directamente sobre la «base de datos». Con la expresión base de datos estamos mencionando a los depósitos electrónicos de datos e información, lo que implica: una organización electrónica de datos e información; un sistema de manejo de base de datos; un control que permite a los usuarios ingresar al mismo, de acuerdo a sus derechos de acceso; una administración o manejo de datos; un

diseño de base de datos y de su estructura así como la selección e implementación del software que permite operarlo» (Villalba, 1988, pág.75).

Una base de datos es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada, para la resolución de un problema planteado en una consulta...La base de datos está formada por tanto, por un conjunto de documentos. Estos documentos pueden ser objeto de propiedad de un tercero y éste tener derechos sobre ellos (conforme: Núñez, ob., cit., pág. 86).

4.3.3.- Suejto Activo

El tipo penal no hace referencia a condición o cualidad específica en el agente, por lo que en principio podemos establecer que se trata de un sujeto activo genérico. En tal sentido, Mazuelos (op., cit., pág. 273), señala que sobre el autor no pesa ningún deber especial, de ahí que se desestime este delito como un delito de infracción de un deber que requiere para su configuración típica de un deber especial sobre el agente

Pero por otro lado, sin que ello signifique variación del tipo, generalmente encontramos en estas figuras delictivas, la presencia de un criminal preparado o especializado que posee el conocimiento y la habilidad necesarios para el manejo de los sistemas informáticos, de allí el incremento de la sofisticación del ataque. Pero ello no es decisivo, ya que en el aspecto de la coautoría o autoría mediata puede concurrir la acción de un sujeto especializado con uno no especializado. Ej. Utilizar a un menor de edad para lograr el acceso al sistema, ante la falta de conocimiento técnico del agente.

Hay quienes sostienen también que se trata de un "delincuente de cuello blanco", conforme a la clasificación introducida por el criminólogo norteamericano Edwin Sutherland en 1943, en razón a las peculiaridades del delito y el status socio-económico del agente, cuya criminalidad se explica no necesariamente por carencias económicas, sino por ambición (e incluso por aventura).

La figura agravada sí reclama un sujeto activo específico, siendo el que obtiene información privilegiada en razón a su cargo.

Se habla aquí de los denominados **piratas informáticos o hackers**, que son las personas que entran sin autorización al interior del sistema del computador. Su ingreso, siendo voluntario, puede deberse a una finalidad de obtener provecho económico, a un afán aventurero, curiosidad, etc. Las modalidades pueden ser variadas, pudiendo acceder por vía remota, instalaciones fijas, correo electrónico, etc.

4.3.4.- Sujeto Pasivo

Es genérico. Lo será el titular del derecho informático afectado, es decir, el titular de la base de datos, sistema o red de computadoras. Puede ser persona jurídica o natural, e incluso el Estado.

4.3.5.- Elementos Materiales

a) **Base o banco de datos**; la manipulación rápida y eficiente y el almacenamiento de volúmenes crecientes de información, caracterizan una nueva etapa de la sociedad en la cual aquélla adquiere valor de mercancía. La emergencia y fundamentación de una industria de bancos de datos es uno de los signos distintivos de esta evolución.

Un servicio de banco de datos es un conjunto organizado de bases de datos, accesibles en línea (directamente desde una computadora) como servicio comercial, para la consulta de datos de la más diversa índole.

Esa nueva industria (que ha originado una nueva "era de la información"), pone en movimiento diversos protagonistas: los productores de bases de datos: instituciones científicas, universitarias, profesionales o empresas que estructuran y actualizan datos concernientes a su área de actuación; los distribuidores: empresas que disponen de gran capacidad de cómputo orientada a la prestación de servicios de consulta; los operadores de redes de transmisión, sean telefónicas o redes especiales de transmisión de datos. En ocasiones, entre el proveedor de los datos y el usuario final actúa una oficina de servicios de información, es decir, entes públicos o privados que facilitan el acceso a bancos de datos.

En la creación de bancos de datos, la información, que hasta ahora ha sido, en su mayor parte, un bien "libre", se hace accesible

por un precio. La apropiación privada sustituye así a la disponibilidad pública, y explica la elaboración de teorías jurídicas tendientes a fundamentar, como se ha visto, la propiedad de la información en sí.

Desde el punto de vista legal, la constitución de bancos de datos suscita cuestiones en cuanto a los derechos de los productores y su eventual conflicto con los autores de las obras que fueren citadas o indexadas.

Los principales problemas que se plantean (conforme: Carlos Correa, ob., cit., pág. 300, Núñez, ob., cit., pág. 86) son:

1) el derecho de los titulares del material almacenado en la base de datos, y la necesidad o no de su autorización para que entren a formar parte de la misma; teniendo en cuenta que la información contenida en el material podrá ser transmitida una vez archivada, a distintos usuarios a través de un servicio de transmisión de datos interconectado telemáticamente. La divulgación de información no autorizada por parte del gestor de base de datos, puede originar daños al titular del material incorporado sin consentimiento en esa base de datos; dependiendo de la naturaleza de la información el perjuicio causado podrá variar, ya sea que se trate, por ejemplo, de información económica y financiera de las empresas o de los datos personales de ejecutivos.

2) Una segunda cuestión a plantear son las obligaciones que asumen los gestores o responsables de las bases de datos al suministrar información correcta y en forma oportuna. En determinados tipos de banco de datos (como en el de carácter legal) es de fundamental importancia que la información sea vigente y llegue en forma oportuna; por cuanto una información derogada o no vigente puede ocasionar daños a los usuarios.

3) Otra cuestión a plantear son las medidas que debe tomar el Administrador o Gestor de la Base de Datos con respecto a la seguridad de los sistemas informáticos, con la finalidad de evitar el uso indebido de ellos o el conocimiento no autorizado de la información contenida (facultad de quien administra el banco de datos de incorporar material protegido), lo que puede ocasionar perjuicios o daños a los titulares de la información o materiales almacenados en la base de datos.

4) Otro aspecto es el derecho de los productores de bases de datos sobre su sistematización. Mas aún, la circunstancia de que el computador "elabore" interrelaciones y sistematizaciones ha llevado a la discusión sobre en qué medida los trabajos "creados" por la máquina pueden ser protegidos por copyright.

b) **Sistema o red de computadoras**; se hace referencia al software o soporte lógico del computador. Puede corresponder a un sólo sistema o estar interconectado a una red de varios ordenadores (utilizar por ejemplo la internet).

El software es el conjunto de instrucciones o expresiones que tienen como finalidad dotar al computador de la capacidad de actuación determinando sus posibilidades de uso y aplicaciones concretas. Es una creación intelectual susceptible de convertirse en un bien inmaterial o incorporal. Este bien inmaterial es objeto de derechos y de la protección jurídica. Por otra parte en aplicación del artículo 886 del Código Civil, también son bienes muebles para efectos de su tráfico jurídico (Núñez, ob., cit., pág. 28).

c) **Acceso indebido**; involucra la inclusión de un elemento normativo en el tipo, regido fundamentalmente por el dolo (de ello se desprende que un error sobre el carácter "indebido", de la utilización o ingreso al sistema, ha de determinar un error de tipo)

Al respecto, la ley establece dos modalidades del acceso ilegítimo: **utilización o ingreso indebido**.

La utilización indebida implica el uso abusivo, no permitido o excesivo del sistema o base de datos; mientras que en el ingreso indebido el agente se introduce, abre sin permiso el sistema o base de datos.

El consentimiento aparece en este delito como una causa de atipicidad de la conducta.

El tipo penal precisa la conducta del agente que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras (o cualquier parte de la misma), con la finalidad de: diseñar (crear), ejecutar (dar aplicación) o alterar un esquema (soporte lógico; soft-

ware) u otro similar; o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos.

4.4.- Tipo subjetivo de los injusto

El tipo es eminentemente doloso. El agente actúa con plena conciencia y voluntad en su ingreso indebido al banco de datos o sistema o red de computadoras, siendo su finalidad la de diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos.

Por ello, bien dice Tiedemann, que estos hechos de ninguna manera pueden ser entendidos como errores involuntarios, ya que son realizados por personas que generalmente están familiarizadas y se encuentran especializadas en el trabajo con computadoras y que fácilmente pueden conocer como entrar en los archivos de datos de cualquiera (ob., cit.).

4.5.- Fraude Informático

El tipo contenido en el artículo 207-A, desde su perspectiva subjetiva, determina una clasificación de la conducta, que incide directamente sobre la penalidad. Ello en cuanto el sujeto actúe con ánimo de lucro o no.

En el simple intrusismo, descrito en la primera parte del referido artículo, el tipo no exige ninguna determinación crematística, pudiendo el agente actuar motivado por cualquier otro tipo de circunstancias subjetivas, como la aventura, la curiosidad, etc. pero por afectar derechos patrimoniales del titular, será imputado. Mientras que en la segunda parte de la figura en comentario el tipo exige que el agente haya actuado con el fin de obtener un beneficio económico.

Esta variación de la finalidad perseguida por el agente, es lo que determina la presencia del denominado "fraude informático", que en esencia viene a ser una modalidad del intrusismo informático motivado por animus lucrandi, lo que denota la presencia de un tipo de tendencia interna trascendente.

El delito de fraude informático, que también es conocido como "estafa informática", corresponde a un tipo de mera actividad, bastando sólo la conducta de intrusismo, sin necesidad que se produzca algún resultado material.

4.6.- Tipo imperfectamente realizado

Tratándose de tipos de mera actividad, no es posible la configuración de la tentativa. La consumación es instantánea.

4.7.- Autorría y participación

Dada su característica típica, son posibles de configurar todas las diferentes formas de autoría y coautoria. La instigación y la complicidad son también perfectamente posibles (el que financia, el que induce, el que presta los equipos, el que aporta los datos o claves necesarias, etc.).

4.8.- Tipo agravado

Conforme lo establecido por el art. 207-C, el tipo se agrava cuando:

a) El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

Muchas veces el agente abusa de su posición obteniendo informaciones que generalmente no son de dominio público, ello en atención a su cargo, que determina una situación especial o laboral estratégica de manejo de información sensible (fundamental).

b) El agente pone en peligro la seguridad nacional.

Ello es una previsión muy importante, y aunque parezca de ciencia ficción, la introducción del hacker a sistemas computarizados tan sensibles y estratégicos, como los que corresponden al sistema de defensa, puede conllevar graves daños a la seguridad nacional. Por ejemplo, interceptar y publicar en internet de manera indebida, los planes estratégicos para la lucha contra subversiva o el combate al narcotráfico, amén de los datos que corresponden a la seguridad exterior de la república.

4.9.- Pena

En la figura básica de intrusión, cuando el fin no es el lucro, la pena será privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, realizando la conducta de fraude informático, la pena aplicable será privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

5.- Sabotaje Informático

5.1.- Presentación de la norma

Artículo 207-B: El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadora o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

5.2.- Bien Jurídico protegido

El patrimonio, desde la perspectiva de la titularidad del derecho y la capacidad de disposición que tiene el propietario sobre la base de datos y del sistema o red de computadoras, como ya se anotó en el estudio del tipo precedente.

5.3.- Tipo objetivo de lo injusto

5.3.1.- Acción Delictiva

La conducta en el sabotaje informático se manifiesta fundamentalmente en el daño o destrucción por parte del agente, de datos y programas del ordenador.

El tipo penal describe la conducta de intrusismo de quien, indebidamente, utiliza, ingresa o interfiere, una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma, **con el fin** de alterarlos, dañarlos o destruirlos. Para la configuración típica sólo basta que el ingreso sea ilegítimo.

De acuerdo a la redacción típica, en su extremo de realización mínimo, el tipo no requiere necesariamente el daño material realizado u objetivado, lo que permite apreciar que, entendido así, el tipo se repre-

senta como uno de peligro. Evidentemente, el resultado material también resulta acogido por el tipo, sin variar la tipicidad.

La consumación se verifica con la mera actividad instrusista animada por la intencionalidad dañosa que señala el tipo.

5.3.2.- Objeto material de la acción

El soporte lógico del sistema informático (software) y la base de datos.

5.3.3.- Sujeto Activo

Genérico, con las características ya tratadas. Podemos hablar aquí de los **crackers**, nombre dado al pirata informático, que ingresa al sistema computacional, con la finalidad de destruir información. Su finalidad puede ser la de robar información produciendo destrozos o la de desproteger todo tipo de programas, con lo que quedan expuestos al daño.

5.3.4.- Sujeto Pasivo

También genérico. Pueden ser personas naturales como jurídicas e incluso el mismo Estado.

5.3.5.- Elementos materiales

a) Base de datos.
b) Sistema, red o programa de computadora (software).
c) Acceso indebido.
d) **Acción delictiva dañosa;** el sabotaje informático inside fundamentalmente en el daño o destrucción por parte del agente, de datos y programas del ordenador.

El tipo penal describe la conducta de intrusismo de quien, indebidamente, utiliza, ingresa o interfiere, una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma, **con el fin** de alterarlos, dañarlos o destruirlos.

La acción puede realizarse mediante "Bombas Lógicas" "bombas cronológicas" o "Logic Bombs", que consiste en introducir en un progra-

ma normal, un conjunto de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada, se ejecuten automáticamente, desencadenando el borrado o la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema o paralizaciones intermitentes.

También puede emplearse la denominada "rutina cáncer", mediante la introducción al sistema de los denominados **virus informáticos**, que a decir de Ferreyra, es todo aquel software código o programa que al ser ejecutado altera la estructura del software del sistema y destruye programas o datos sin autorización y conocimiento del operador (ob., cit.). Son instrucciones que se regeneran o autorreproducen. Igualmente puede utilizarse el llamado **"gusano"**, cuyo origen es similar al virus informático y se usa infiltrándolo en programas normales para modificar o destruir la información. Se diferencia del virus en que no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá, puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero de una cuenta a otra de manera ilícita.

5.4.- Tipo subjetivo de lo injusto

La acción es eminentemente dolosa. La conducta del cracker se dirige fundamentalmente a dañar, alterar o destruir el soporte lógico (tendencia interna trascendente). Si la conducta del sujeto se orienta a dañar sólo la parte externa (hardware) del ordenador, no podemos hablar de delito informático, sino de daños.

5.5.- Tipo imperfectamente realizado

Dentro de las características subjetivas ya anotadas en el estudio del tipo precedente, la tentativa resulta imposible.

5.6.- Autoría y participación

Tanto la autoría como la participación son configurables.

5.7.- TIPO AGRAVADO

Conforme a lo dispuesto por el art. 207-C, el tipo se agrava cuando:

a) El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
b) El agente pone en peligro la seguridad nacional.

5.8.- Pena

La pena aplicable, en la figura simple, es privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

BIBLIOGRAFÍA

BACIGALUPO, Enrique "Estudios sobre la parte especial del Derecho Penal", 2da Edición, Madrid, 1994.

BAJO FERNANDEZ, Miguel "Manual de Derecho Penal. Parte Especial. Delitos Patrimoniales Económicos", Edit. Centro de Estudios Ramón Areces S. A., Madrid, 1991.

BLOSSIERS MAZZINI, Juan José y CALDERÓN GARCÍA, Silvia B. "Los Delitos Informáticos (en la Banca)", Editora Rao S.R.L., Lima 2000.

CORREA, Carlos M. y Otros "Derecho Informático" Ediciones Depalma, Buenos Aires 1987.

CREUS, Carlos "Derecho Penal: Parte Especial", Tomo 1, Tercera Edición, Editorial Astrea, Buenos Aires 1990.

DAVARA, Miguel Angel "Derecho Informático", Editorial Aranzandi, España 1993.

DEL RIO C. J. Raymundo "Derecho Penal: Delitos Especiales", Tercer Tomo, Editorial Nascimento, Santiago de Chile, 1935.

EZAINE, Amado "Diccionario de Derecho Penal" A.F.A Editores Importadores S.A

FALCONI PÉREZ, Miguel	"Protección Jurídica a los Programas de Computación", Edino 1991 - Lima.
FERREYRA CORTEZ, Gonzalo	"Virus en las Computadoras", Editorial Macrobit, México 1990.
FONTAN BALESTRA, Carlos	"Derecho Penal: Parte Especial", Decimo Cuarta Edición, Abeledo Perrot, Buenos Aires Argentina 1994.
LISZT, Franz Von	"Tratado de Derecho Penal", Madrid, 1916.
MAZUELOS COELLO, Julio F.	"Los Delitos Informáticos: Una Aproximación a la Regulación del Código Penal Peruano", en: Revista Peruana de Doctrina y Jurisprudencia Penales 2, Instituto Peruano de Ciencias Penales, Grijley, Lima 2001.
MUÑOZ CONDE, Francisco	"Culpabilidad y prevención", en: Cuadernos de Política Criminal No 12, Lima 1980.
MUÑOZ CONDE, Francisco	"Teoría General del Delito", Editorial Temis, Bogotá 1990.
MUÑOZ CONDE, Francisco	"Derecho Penal: Parte Especial, Undécima Edición, Edi. Tirant lo Blanch , Valencia 1996.
PEÑA CABRERA, Raúl	"Tratado de Derecho Penal: Parte Especial II - A ; Delitos contra el patrimonio", Ediciones Jurídicas Lima - Perú 1995.
PORTE PETIT, Celestino	"Ensayo Dogmático del Delito de Rapto Propio", 2° Edi., Edit. Trillas, México 1984.
PRADO SALDARRIAGA, Víctor	"Derecho Penal Jueces y Jurisprudencia (Parte General), Palestra Editores, Lima 1999.
QUERALT JIMÉNEZ, Joan J.	"Derecho Penal Español: Parte Especial, Tercera Edición, Jose Maria Bosh Editor, Barcelona 1996.
QUINTANO RIPOLLES, Antonio	"Tratado de la parte especial de Derecho penal, T. II, De. Revista de Derecho Privado, Madrid, 1985.

QUINTERO OLIVARES, Gonzalo "Comentarios a la Parte Especial del Derecho Penal", Arazandi Editorial, Pamplona España, 1996.

ROJAS VARGAS, Fidel "Delitos Contra el Patrimonio", Volumen I, Grijley, Lima 2000, primera edición.

ROY FREYRE, Luis E. "Derecho Penal Peruano", Tomo III, Parte Especial, Delitos contra el Patrimonio, Instituto Peruano de Ciencias Penales, Lima - Perú, 1983.

TIEDEMANN, Klaus "Criminalidad Mediante Computadoras", En Poder Económico y Delito, Editorial Ariel, S.A. Barcelona 1985.

VILLALBA, Carlos Alberto "La Protección de los Programas de Computación y de los Bancos de Datos, Editorial OMPI, Lima 1988.

VILLAVICENCIO TERREROS, "Código Penal", 2da Edición, Editorial Grijley, Lima - Perú.

ZAFFARONI, Eugenio Raúl "Tratado de Derecho Penal. Parte General", T. V, Ediar, Buenos Aires, 1983.