BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE
DEPARTAMENTO DE ESTUDIOS, EXTENSIÓN Y PUBLICACIONES

DELITOS INFORMÁTICOS
EN LA LEGISLACIÓN DE ESPAÑA, FRANCIA, ALEMANIA E ITALIA.

DEPESEX/BCN/SERIE ESTUDIOS
AÑO XIV, Nº 296

SANTIAGO DE CHILE
JULIO DE 2004

TABLA DE CONTENIDOS

I.- INTRODUCCIÓN 1

II.- MARCO TEÓRICO 2

2.1 CONCEPTO DE DELITO INFORMÁTICO. 2
2.2 BIEN JURÍDICO PROTEGIDO. 3
2.3 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS. 4
2.3.1 Conductas lesivas a la confiabilidad de la información 6
2.3.2. Conductas lesivas a la integridad de la Información 7
2.3.3 Conductas lesivas a la disponibilidad 7
2.4 SUJETOS. 7
2.4.1 El Sujeto Activo 7
2.4.2 El Sujeto pasivo 8

III - LEGISLACIÓN EXTRANJERA 8

3.1 ESPAÑA 8
3.1.1 Daños en sistemas o elementos informáticos y en datos, programas o documentos electrónicos (Sabotaje informático) 9
3.1.2 Acceso Ilícito a Sistemas Informáticos 12
a. Accesos ilícitos a datos calificables de "Secreto de Empresa" 12
3.1.3 Protección Penal de los Programas de Ordenador 16
a. Piratería de Programas de Ordenador 16
b. Adquisición o recibimiento de copias no autorizadas de programas de ordenador 20
c. Conductas relacionadas con la desprotección de programas de ordenador 22
3.1.4 Utilización Ilegítima de Terminales de Comunicación. 22
3.1.5 Los Ilícitos patrimoniales realizados por medio del sistema informático: 24
a. Estafa por medios informáticos. 24
b. Apoderamiento de dinero utilizando tarjetas de créditos. 26
c. Abuso de Cajeros Automáticos. 26
d. Utilización de Tarjetas de Cajeros Automáticos y Fuerza en las Cosas 28
3.1.6 Infracciones a la Intimidad y Privacidad. 29
3.2 FRANCIA 31
3.2.1 Acceso fraudulento a un sistema de elaboración de datos. 33
3.2.2 Sabotaje informático 33
3.2.3 Destrucción de datos. 33
3.2.4 Asociaciones para cometer delitos informáticos. 34
3.2.5 Falsificación y uso de documentos electrónicos falsificados. 35
3.3 ALEMANIA. 35
3.3.1 Espionaje de datos. 36
3.3.2 Estafa informática. 36
3.3.3 Falsificación de datos probatorios. 39
3.2.4 Alteración de datos. 40
3.3.5 Sabotaje informático 40
3.4 ITALIA. 41

3.4.1 Acceso abusivo a un sistema informático o telemático (artículo 615 tercero).....41
3.4.2 Difusión de programas dirigidos a producir daños o interrumpir un sistema informático o telemático (artículo 615 quinto).....41
3.4.3 Atentado contra un sistema informático o telemático de utilidad pública (artículo 420).....41
3.4.4 Abuso de la calidad de operador de sistema.....42
3.4.5 Detentación y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos (Artículo 615 cuarto).....42
a. Difusión de programas dirigidos a dañar o interrumpir un sistema informático (Artículo 615 quinto).....42
b. Violación de la correspondencia electrónica (articulo 616).....42
c. Intercepción abusiva. (Artículo 617, cuarto, quinto).....42
3.4.6 Falsificación informática (617 sexto).....43
3.4.7 Espionaje informático.....43
3.4.8 Fraude informático (Artículo 640 tercero).....43
3.4.9 Ejercicio arbitrario de la propia razón con violencia sobre programas informáticos (Artículo 392).....43
IV. CONCLUSIONES.....44
V. SELECCIÓN BIBLIOGRÁFICA.....46

Resumen.

De acuerdo con el desarrollo doctrinal del tema, el concepto de delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, etc., como aquellas conductas que recaen sobre herramientas informáticas propiamente tales como programas, ordenadores, etc. En el primer supuesto el bien jurídico protegido en cada caso será el que corresponda a la naturaleza de la infracción cometida. En el segundo, será la información entendida como proceso que englobe el almacenamiento, el tratamiento y la trasmisión. Las propuestas de regulación de organismo y entidades internacionales han seguido normalmente los criterios clásicos, y en similares términos ha sido la respuesta normativa en el derecho comparado.

Se analiza la legislación de España, Francia, Alemania e Italia. En España, el legislador siguiendo la técnica legislativa de la complementación, amplió las tradicionales figuras delictivas existentes con una categoría nueva de objetos sobre los cuales puede recaer la acción del sujeto activo, así, incluyó los datos informáticos, el software o un programa informático como trabajo susceptible de protección. En Francia, el legislador a través de la técnica legislativa especial, criminalizó la conducta por medio de un juego de disposiciones de la misma clase, castigando las especialidades de un particular uso indebido, o abuso informático, salvo el fraude informático cubierto por el artículo 441-1. En Alemania, el legislador utilizó dos técnicas legislativas, la de la complementación para la modificación de las figuras clásicas y, la de la extensión que elabora una figura especial, paralela e inspirada en la existente, pero con relación a bienes nuevos como los sistemas informáticos. El legislador italiano, a través de la reforma del Código Penal, incluyó los delitos informáticos, mediante una sistemática extensiva, pero con una estructura distinta de la figura tradicional.

DELITOS INFORMÁTICOS EN LA LEGISLACIÓN DE ESPAÑA, FRANCIA, ALEMANIA E ITALIA.

Estudio elaborado por Patricia Canales con la colaboración de Virginie Loiseau, de la Sección Estudios de la Biblioteca del Congreso Nacional.

I.- INTRODUCCIÓN

Se hace evidente la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, las comunicaciones, los procesos industriales, las investigaciones, seguridad, sanidad, etc., son aspectos cada día más dependientes del desarrollo de la tecnología informática.

Sin embargo, junto al avance de la tecnología informática, han surgido una serie de comportamientos ilícitos llamados genéricamente delitos informáticos, que adoptan formas muy distintas, incluido el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicios, que pueden ser cometidos en cualquier lugar del mundo contra el resto del mundo y en cualquier momento. Estos delitos contra los sistemas de información amenazan la creación de una sociedad más segura y de un espacio de libertad, seguridad y justicia.

Este trabajo contiene un marco teórico y un análisis de la legislación de España, Francia, Alemania e Italia.

II.- MARCO TEÓRICO

2.1 CONCEPTO DE DELITO INFORMÁTICO.

De acuerdo con el desarrollo doctrinal del tema, el concepto de delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad, etc., como aquellas que recaen sobre herramientas informáticas propiamente tales como programas, ordenadores, etc.

El primer supuesto lleva a una ampliación de la forma en que un delito pueda cometerse. En este caso, el aceptar el uso de la computadora como instrumento delictivo no importa aplicar analogía de ninguna especie, sino adaptar la figura penal a los avances de la tecnología. El límite de esta interpretación del tipo penal se encuentra en los supuestos en que el legislador previó específicamente un medio determinado, como es el caso de los delitos calificados, o en los que la estructura del delito no permita el empleo de ese medio. Sin embargo, la enunciación genérica de una serie de medios dentro de los cuales tenga cabida el uso del ordenador o se permita expresamente el uso de cualquier medio, no otorga al delito el carácter de "informático", sin perjuicio de que se hable de un delito relacionado con la informática.

Dentro de este tema, donde el computador se usa como medio o instrumento se encuentra la doble contabilidad llevada por ordenador con fines de evasión fiscal, la creación de registros falsos con la finalidad de cobrar créditos inexistentes, jubilaciones, sueldos, etc.

El segundo supuesto, donde la informática es objeto del delito, hay que diferenciar el "*hardware"* del *"software",* señalando que al primero son generalmente aplicables las normas tradicionales ya que no constituye una nueva forma de propiedad. Distinto es el caso del software y de la información almacenada en una computadora, pues estos constituyen formas intangibles y no siempre tienen cabida en las instituciones tradicionales del Derecho. Hay que señalar que en las situaciones delictuosas en las que los materiales informáticos no tienen otra función que la de simple objeto, no se configura un delito informático, ya que al tipificarse un

delito informático lo que se busca es tutelar el contenido de información de un sistema informático, y no el hardware en sí mismo.

Se considera delito informático la reproducción ilícita de obras de software, de bases de datos o de topografías de semiconductores. Hay situaciones en que se dan los dos supuestos, es decir el ordenador se usa como instrumento y es a la vez el objeto sobre el cual recae la acción delictiva, como es la destrucción de datos mediante un programa de virus informático.

En cuanto a la definición Davara Rodríguez[1] lo entiende 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 hardware o software"*.

Un grupo de expertos de la OCDE, definió, en 1983, el delito informático como *"cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos"*. Esta definición amplia, se ha considerado como ventajosa, ya que abarca no sólo el delito informático sino toda la delincuencia relacionada con la informática[2] y las nuevas tecnologías.

2.2 BIEN JURÍDICO PROTEGIDO.

En los supuestos en que la informática es el medio utilizado para delinquir, el bien jurídico protegido en cada caso será el que corresponda a la naturaleza de la infracción cometida: la intimidad, la propiedad, la fe pública, etc.

---

[1] Citado por Pablo Andrés Pañazzi en "*Delitos Informáticos*", p. 36.

[2] De acuerdo con la doctrina la categoría denominada "delincuencia informática, es útil para determinar de lege ferenda qué conductas cometidas por medio de sistemas de procesamientos de datos, o en éstos, pueden lesionar bienes jurídicos vinculados a derechos individuales y así proceder a su tipificación, y de lege data, permite al operador jurídico determinar cuándo se encuentran ante una conducta antijurídica, por haber lesionado tales bienes jurídicos o haberlos puestos concretamente en peligro.

Cuando se trate de delitos que recaen sobre objetos informáticos propiamente dichos, el bien jurídico protegido será la información entendida como proceso que englobe el almacenamiento, tratamiento y transmisión. Así, la información se considera como un valor económico de la actividad de la empresa dedicada a la información.

En la determinación si se trata de un bien jurídico penal individual o de carácter colectivo, se considera que se está ante un interés social vinculado a la actividad empresarial, por lo tanto se encontraría situado dentro de los llamados delitos socio-económicos y por ello sus repercusiones transcenderían a las bases del sistema socio-económico, esto es, se trataría de un bien jurídico colectivo. No obstante, pueden resultar implicados en determinados supuestos, intereses patrimoniales individuales, que en éste caso serían los de los propietarios de la información contenida en los sistemas de tratamiento automatizado de datos.

En concreto, parte importante de la doctrina ha considerado la información como un bien jurídico intermedio o de referente individual, que se define como intereses colectivos tutelados penalmente en forma conjunta con bienes de los particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque. Por ejemplo, la pureza del ambiente y la vida o salud personal, o el atentado contra la seguridad del tráfico y la simultánea puesta en peligro de la vida o integridad de la persona.

2.3 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

La Convención de Delitos Informáticos del Consejo de Europa de 2001, clasifica las conductas lesivas a la información en cuatro tipos:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.- Sanciona el acceso y la intercepción ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
b) Delitos de fraude informático.- Falsificación y fraude computacional
c) Delitos por su contenido.- Producción diseminación y posesión de pornografía infantil.

d) Delitos relacionados con la infracción de la propiedad intelectual y derechos afines.- La amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor.

La Unión Europea, en la Propuesta de Decisión-Marco del Consejo Relativa a los Ataques de los que son Objeto los Sistemas de Información, de agosto de 2002, identifica las siguientes amenazas:

a) Acceso no autorizado a sistemas de información, que incluye la "piratería" informática;
b) Perturbación de los sistemas de información, como la "denegación de servicio";
c) Ejecución de programas perjudiciales que modifican o destruyen datos, incluye virus, bombas lógicas y gusanos;
d) Interceptación de las comunicaciones, denominada intromisión (sniffing);
e) Declaraciones falsas, se trata de la usurpación de la identidad de una persona en Internet, se llama "spoofing" (modificación de datos).

Las Naciones Unidas, reconoce los siguientes tipos de delitos informáticos.

1. **Fraudes cometidos mediante manipulación de computadoras:** a) Manipulación de datos de entrada; b) manipulación de programas; c) manipulación de datos de salida; d) fraude efectuado por manipulación informática.
2. **Falsificaciones informáticas:** a) como objeto, se alteran datos de los documentos almacenados; b) como instrumentos.
3. **Daños o modificaciones de programas o datos computarizados:** a) Sabotaje informático; b) virus; c) gusanos: d) bomba lógica o cronológica.
4. **Falsificaciones informáticas:** a) Acceso no autorizado a sistemas o servicios; b) piratas informáticos o hackers; c) reproducción no autorizada de programas informáticos.

Por su parte la doctrina analiza los atentados contra la información a partir de sus propiedades esenciales: **confidencialidad**, **integridad** y **disponibilidad**.

2.3.1 Conductas lesivas a la confiabilidad de la información

Entre estas se encuentran:

1. **El Espionaje Informático (Industrial o Comercial).** Con los términos industrial y comercial se pretende delimitar esta categoría, excluyendo bienes jurídicos distintos como sería el caso de delitos contra el Estado y la defensa nacional o contra la intimidad. Debe entenderse como la obtención con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio. Dentro de los comportamientos que pueden ser incluidos en esta descripción se identifican los siguientes: La fuga de datos (Data Leakage), que las empresas o entidades guardan en sus archivos informáticos; las puertas falsas (Trap Doors), consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas. Las "llaves maestras" (Supperzapping) que implica el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información. El pinchado de líneas (Wiretapping), que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se trasmiten las informaciones procesadas. La apropiación de informaciones residuales (Scavenging) que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

2. **El Intrusismo informático.** Se define como la mera introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellos. A primera vista pareciera que el Sabotaje Informático y el Intrusismo fueran comportamientos idénticos, sin embargo el elemento subjetivo delimita estos comportamientos. En el primer supuesto, la intencionalidad del agente es obstaculizar el funcionamiento de un sistema informático, en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la producción de perjuicio, que se produzca, es ajeno al comportamiento aunque es evidente que lo agrava.

2.3.2. Conductas lesivas a la integridad de la Información

Consisten en el acceso directo u oculto no autorizado a un sistema informático mediante la introducción de nuevos programas denominados virus, "gusanos" o "bombas lógicas". El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema, recibe el nombre de "sabotaje informático".

2.3.3 Conductas lesivas a la disponibilidad

Las bombas lógicas y los virus informáticos pueden afectar transitoriamente la disponibilidad de la información, sin destruirla. Otro de los mecanismos que pueden impedir el acceso a un sistema de información por parte de los usuarios legítimos, son los denominados "spam" o el "electronic-mail bombing", que consisten en el envío de cientos de miles de mensajes de correo electrónico no solicitados o autorizados, para bloquear los sistemas.

2.4 SUJETOS.

2.4.1 El Sujeto Activo

Las personas que cometen los delitos informáticos son aquellas que poseen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando no desarrollen actividades que faciliten la comisión de este tipo de delitos. Se ha dicho que son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico. Los que los diferencia entre sí es la naturaleza del delito cometido. 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.

2.4.2 El Sujeto pasivo

Es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. No ha sido posible conocer la verdadera magnitud de estos delitos, ya que la mayor parte de ellos no son descubiertos o no son denunciados a las autoridades responsables, a lo que se añade el temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que pudiera ocasionar.

III - LEGISLACIÓN EXTRANJERA

3.1 ESPAÑA.

El Código Penal de 1995 contiene normas específicas relativas a conductas que tienen a sistemas o a elementos informáticos como objeto de ataque o como instrumento del delito. A los delitos contra los sistemas informáticos que afecten a elementos físicos del mismo, se les aplicará las reglas destinadas a comportamientos semejantes dirigidos contra otros objetos. Así, al hurto, robo, apropiación indebida, estafa, se sancionarán de acuerdo con los criterios interpretativos de cada uno de ellos. Lo mismo sucede con los ficheros de información o con los programas contenidos en soportes de almacenamiento masivo cuando es el objeto físico en el que se encuentran grabados (disquete, cinta, disco duro, CD- ROM, etc.).

La situación es radicalmente distinta cuando de trata de comportamientos relacionados con elementos lógicos del sistema, que afecten exclusivamente a los ficheros y programas, sin incidencia en los elementos físicos del sistema informático. Aunque estas conductas pueden producirse también por medios físicos (destrucción de ficheros de datos rompiendo el disco en el que se encuentran), generalmente se llevarán a cabo exclusivamente mediante procedimientos informáticos, copiando, borrando, manipulando, accediendo ilícitamente al sistema, transmitiendo la información o las instrucciones que contienen los datos, los ficheros o los programas afectados.

Considerando la variedad de posibilidades que pueden darse, el análisis se hará distinguiendo cinco grupos: 1) Borrado, alteración o utilización de datos, programas o documentos electrónicos, denominado comúnmente sabotaje informático, debe ser analizado desde la perspectiva de los daños, incluyéndose los causados en los propios sistemas o elementos físicos de los mismos, 2) acceso ilícito a sistemas informáticos, se incluye el espionaje electrónico, el apoderamiento de datos, ficheros y programas e incluso los daños cuando este sea el fin que se pretenda y se cause. Cuando el acceso ilegítimo es la vía utilizada para obtener un beneficio patrimonial propio o de tercero (transferencias electrónicas de fondos, por ejemplo) se analizará el hecho en los delitos cometidos a través del sistema informático; 3) protección de programas de ordenador, conductas que recaen en la propiedad intelectual; 4) utilización ilegítima de sistemas o elementos informáticos, modalidad de uso prevista expresamente para los terminales de comunicación; 5) vulneración de la intimidad.

3.1.1 Daños en sistemas o elementos informáticos y en datos, programas o documentos electrónicos (Sabotaje informático)

Los daños pueden afectar los elementos físicos del sistema o los elementos lógicos.

En el primer caso, se aplica el tipo básico de daños del artículo 263[3] que dispone: *"Si se causare daño en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas"*.

El segundo caso, se aplica el Art. 264.2, en el que se recoge como modalidad agravada de daños la conducta de quien por cualquier medio *"destruya, altere, utilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"*.

[3] El Código Penal ha sido modificado por la Ley Orgánica 15/2003 que entrará en vigor el día 1º de octubre de 2004. En este trabajo, cuando sea necesario se incluirán las dos redacciones, esto es, la vigente hasta el 30 de septiembre y la nueva, que regirá a partir del 1º de octubre de 2004.

De acuerdo con esta disposición el objeto material del delito está constituido por: datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, cuya característica común es que no pueden ser leídos o percibidos directamente, necesitándose la ayuda de máquinas capaces de interpretar las señales digitales que lo integran. Datos, son las unidades básicas de la información, cualquiera que sea su contenido (un número, una palabra, un sonido, una imagen) y que al ser procesados dan lugar a la información que resulta de la conexión de dos o más datos. Programas, son las secuencias de instrucciones que se utilizan para el procesamiento de los datos, para la realización de tareas específicas. Los documentos electrónicos, son aquellos en que se recogen los resultados del procesamiento de los datos obtenidos con las distintas aplicaciones. El precepto señala que pueden estar contenidos en redes, soportes o sistemas informáticos, por lo tanto es indiferente que en el momento de la conducta se encuentren recogidos en memoria central o soporte magnético.

En cuanto a la condición de "ajenidad" de los datos, la determinación de a quién pertenecen en exclusiva, puede presentar dificultades, considerando que se trata de elementos en los que es frecuente el uso y la elaboración compartida. En todo caso, estos problemas deben ser resueltos a través de la normativa civil correspondiente.

Respecto a la conducta típica "dañar", centrada en los elementos lógicos, significa destruir, deteriorar, inutilizar o alterar datos, programas o documentos electrónicos. Así está establecido expresamente en el artículo 264.2, a través de una formulación tan amplia que pareciera aceptar implícitamente que pudiera haber otros elementos lógicos en los que recayeran las modalidades de conducta.

Con relación a los daños se discute si es necesario que se altere la sustancia de la cosa y si es necesario que se cause un perjuicio patrimonial efectivo al sujeto pasivo. En cuanto a lo primero, la opinión mayoritaria mantiene la existencia del delito cuando se priva al propietario del valor de uso a que aparecía destinada la cosa dañada, entre otras razones porque la exigencia que se afecte la estructura material del objeto no está contenida en el Código y porque en las referencias a la inutilización (Art. 264.2 y 265) se acogen los casos en

los que simplemente se destruye ese valor. El sector minoritario considera que el delito de daños significa que se afecte la esencia o sustancia de la cosa, de manera que no serían constitutivos del delito los casos en los que permaneciendo inalterada la estructura material del objeto, sólo se lesiona el valor de uso que tiene para su propietario. Un sector intermedio estima que el término "inutilización" es perfectamente congruente con la exigencia de que en los daños se afecte la sustancia, que determine, aún en forma mínima, un menoscabo de la cosa que incide en su propia existencia y suponga una pérdida de valor real independiente de los perjuicios derivados de la imposibilidad de uso, comprendiendo, en todo caso, la pérdida, corrupción o degradación del objeto, así como la alteración o inutilización.

Las referencias del Art. 264.2 a "*por cualquier medio*" o "*de cualquier modo*", conducen a entender que dentro del tipo agravado de la norma se incluyen las conductas dirigidas directamente a dañar ciertos elementos físicos que necesariamente comportarán la destrucción de datos.

Ahora bien, la destrucción, que determina la existencia del delito del Art. 264.2, debe entenderse como desaparición completa y definitiva de los datos, programas o documentos (por cualquier forma: destrucción del soporte, interferencias magnéticas, eliminación de enlaces, etc.), en el sentido que no sea posible la recuperación íntegra de los mismos. La alteración, cualquiera que sea su forma (añadiendo nuevos datos, borrando parcialmente los existentes, etc.), debe suponer una perturbación funcional definitiva, esto es, que los datos acaben teniendo un contenido distinto al original. La inutilización, es equivalente a la desaparición de su capacidad funcional, como puede ocurrir cuando se les protege con una clave de acceso desconocida para el titular. La simple ocultación del fichero, no daría lugar al delito, a menos que lo convierta en irrecuperable. Así, la destrucción, la alteración, la inutilización o el daño han de significar el cambio definitivo de la integridad de los datos, haciendo imposible su utilización o restauración tal y como estaban antes de la realización de la conducta.

Por lo tanto, deberá apreciarse la tentativa cuando el virus, la bomba lógica o el procedimiento utilizado para causar el daño no llega a activarse, o cuando existan copias de

respaldo o copias de seguridad de los ficheros o de los datos dañados, o existan otras copias del programa que permiten su reinstalación. El delito será consumado cuando aún habiendo copias de seguridad, éstas no son idénticas. La cuantía a tomar en cuenta será la del elemento lógico dañado, integrándose en la responsabilidad civil los perjuicios que se deriven de la diferencia de valor entre el fichero destruido y el últimamente salvado.

3.1.2 Acceso Ilícito a Sistemas Informáticos

El hacking es la denominación genérica con la que se hace referencia al acceso no autorizado a sistemas informáticos ajenos utilizando las redes públicas de telefonía o transmisión de datos. Tiene dos modalidades: el directo, que se define como acceso indebido no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional; el indirecto, supone un acceso inconsentido al ordenador o sistema informático como medio para cometer diferentes conductas delictivas. Se castiga con el delito finalmente cometido (Ej. daños, interceptación del correo electrónico, etc.). El Código Penal español no ha previsto ninguna de estas dos modalidades.

Dentro de esta categoría, el Código español contempla el acceso ilícitos a datos calificables de "*secreto de empresa*".

a. Accesos ilícitos a datos calificables de "Secreto de Empresa".

> Artículo 278. *"1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran a los mismos, o empleare alguno de los medios o instrumentos señalados en el artículo 197[4], será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses".*
> *2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren, o cedieren a terceros los secretos descubiertos.*

[4] Artículo 197.1. *"El que, para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros instrumentos o efectos personales o intercepte sus comunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con penas de prisión de uno a cuatro años y multa...".*

3. Lo dispuesto en el presente Artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

Artículo 279. *"La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses".*

Artículo 280. *"El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos Artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses".*

La referencia básica está contenida en el artículo 278.1, si además de descubrir el secreto, el sujeto lo difundiere, revelare o cediere a terceros, será de aplicación el Art. 278.2. Cuando estas conductas se realicen por quien tiene legal o contractualmente obligación de guardar reserva, se aplicará el 279. Si los hechos se realizaren por quien no intervino en el descubrimiento, pero conoce su origen ilícito, se sanciona de acuerdo con el Art. 280.

La disposición del Art. 278.1 se refiere expresamente a datos, documentos electrónicos, soportes informáticos y por remisión al artículo 197.1 a mensajes de correo electrónico, telecomunicaciones o cualquier otra señal de comunicación. Para que opere la protección es necesario que en ellos se contenga un "secreto de empresa", entendiéndose por tal toda información relativa a la industria o empresa que conocen un número reducido de personas y que por su importancia el titular desea mantener oculta. Comprende tanto los relativos a aspectos industriales (procedimientos de fabricación, investigación de nuevos productos o procedimientos, etc.), como comerciales (listas de clientes, tarifas y descuentos, estrategias, etc.) y en general los relativos a la organización interna de la empresa cuyo conocimiento puede afectar a su capacidad para competir (situación financiera, inversiones, relaciones con accionistas, etc.). Se comprenden tanto los que son fruto de las actividades de la propia empresa, su dueño, directivos o empleados, como los procedentes de terceros, que los han cedido a título oneroso o gratuito.

Se sancionan dos conductas: 1) la que consiste en apoderarse por cualquier medio de los datos, de los documentos electrónicos o de los soportes informáticos en los que se encuentra el secreto, o en utilizar los medios del Art. 197.1, donde también se alude al

apoderamiento de elementos lógicos, esto es, mensajes de correos electrónicos y 2) la interceptación de comunicaciones o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Sujeto activo puede ser cualquiera (en el Art. 278.1), sujeto pasivo es el titular de la empresa, cuya capacidad competitiva se ve afectada con la conducta, y que puede ser distinto del propietario de los papeles o datos de los que se apodera el autor.

En cuanto a las conductas, referidas a los elementos lógicos que pueden dar lugar al "apoderarse" que requiere el tipo, se señala que los soportes informáticos son elementos físicos y su apoderamiento no plantea dificultades. La referencia a los datos, documentos electrónicos y mensajes de correo electrónico se hace en la medida en que no se encuentren recogidos en soportes físicos, sino que estén en el sistema directamente (memoria RAM, ejemplo) o, aún grabados en el fichero, su apoderamiento se produce directamente, sin tomar el elemento del hardware en el que se encuentra el archivo, actuando directamente sobre el mismo. En estos casos, las únicas formas posibles de realizar la conducta serían ver los datos directamente en la pantalla, copiarlos en un soporte propio (con o sin destrucción del original) o transmitirlo a otro equipo informático o a una red.

Sin embargo, aun cuando el sentido genérico del vocablo apoderarse[5] es hacerse dueño de una cosa, tanto en el artículo 278.1 como el 197.1, el apoderamiento ha de efectuarse con la finalidad específica de descubrir un secreto, lo que pone de manifiesto que lo determinante no es tomar para apropiarse, sino para acceder al contenido del fichero y conocerlo: hacerse dueño del secreto. Así, se pueden considerar típicos los supuestos en que el sujeto se limita a ver en pantalla el documento o fichero en que se encuentra el secreto de empresa, sin tomar materialmente nada. Tanto la referencia a "apoderarse por cualquier medio", como las situaciones contempladas en el Art. 197.1, de interferencia de telecomunicaciones o utilización de artificios técnicos de escucha y similares, evidencian que basta la captación intelectual del secreto. Se puede añadir, que el apartado 3 del Art. 278 señala que las penas que pudieran corresponder por el apoderamiento de los elementos en donde se encuentra el secreto se

[5] El sentido propio de apoderarse es tomar, coger, aprehender una cosa.

entenderán sin perjuicio de las que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos, lo que corrobora la afirmación.

Las conductas para ser sancionadas deben reunir dos condiciones: 1) que el secreto se descubra como consecuencia de un apoderamiento o una interceptación, de manera que si se llega al conocimiento del mismo por una vía distinta (por error de dirección al enviar el mensaje por correo electrónico, por ejemplo) no se configura el delito; 2) el apoderamiento ha de hacerse "para descubrir un secreto de empresa", elemento subjetivo del injusto que sólo hace típicos los apoderamientos, la utilización de medios técnicos o las interceptaciones que se realicen con esa finalidad.

Aun cuando "descubrir" es conocer una cosa que se ignora, aunque no se haga partícipe de ello a otro, la consumación se produce, sin embargo, con el apoderamiento de los objetos o soportes en donde se contiene el secreto de empresa, o con la utilización de los medios técnicos, aunque el sujeto no llegue a saber o conocer realmente el contenido del mismo. En la práctica, por la naturaleza de su contenido, no será inusual que quien realiza la conducta no esté en condiciones de entender su significado, se trata entonces de un delito de consumación anticipada (delitos de peligro) en el que ésta se adelanta al momento mismo en que el sujeto realiza la acción con el propósito requerido por el tipo. No se exige perjuicio alguno, pero su existencia va implícita en el concepto de secreto y en relación con el bien jurídico protegido.

Ahora bien, el apartado 3 del Art. 278 establece que lo dispuesto en el artículo se entenderá sin perjuicio de las penas que pudieran corresponder por apoderamiento o destrucción de los soportes informáticos. La doctrina ha criticado la norma, porque lo que dice literalmente es que el posible concurso de delitos se producirá sólo en relación con los soportes informáticos, pero no cuando se trata de otros elementos (papeles, documentos escritos, medios audiovisuales, etc.), aunque tengan valor económico. Además cuando se refiere a soportes informáticos, pareciera estar comprendiendo sólo los casos en que hay apoderamiento o destrucción del dispositivo físico en el que se encuentra grabado o recogido el secreto de empresa, con exclusión de aquéllos otros en los que el autor se limita a destruir o

copiar el elemento lógico en sí (borrado de fichero, eliminación de los datos en memoria efímera) Aún así debe entenderse que la posibilidad de concurso se puede producir en relación con cualquier elemento que contenga el secreto de la empresa que tengan valor económico propio.

3.1.3 Protección Penal de los Programas de Ordenador

a. Piratería de Programas de Ordenador

El derecho español protege los programas de ordenador a través de las normas sobre propiedad intelectual contenidas en los artículos 270 y 271 del Código Penal las que deben ser interpretadas de acuerdo a lo dispuesto en la Ley de Propiedad Intelectual.

La definición de programa de ordenador está contenida en el artículo 96. del Texto Refundido de la Ley de Propiedad Intelectual (TRLPI) que establece *"1. se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión o fijación.*
A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este título dispensa a los programas de ordenador".
2. El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia del autor.
3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa, así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.
Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderle por la aplicación del régimen de propiedad industria.
No estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfases".

De esta disposición se desprende que la única condición para que un programa de ordenador pueda ser obra protegida, es que sea original, en el sentido de ser una creación

intelectual propia de su autor. La tutela penal comprende tanto el programa fuente como el programa objeto, la documentación preparatoria, la documentación técnica y los manuales de uso. No alcanza a las ideas y a los principios básicos del programa, incluidos los que sirven de fundamento a sus interfases. En cuanto a estas últimas, lo que se protege son las formas de "expresión" de esas ideas. La delimitación entre "expresión e "ideas", ofrece dificultades para hacerla con claridad, pero es decisiva para determinar los términos de la tutela, en especial el plagio. También están protegidas las transformaciones de los programas de ordenador, lo que permite incluir las versiones sucesivas y los programas derivados. Quedan excluidos de la protección los programas creados con la finalidad de causar efectos nocivos a los sistemas (virus).

Artículo 270 del Código Penal[6]: *"Será castigado con pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.*
La misma pena se impondrá a quien intencionalmente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.
Será castigada con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador".

Artículo 271.[7] *"Se impondrá la pena de prisión de un año a cuatro, multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada*

[6] La disposición ha sido modificada por la Ley Orgánica 15/2003, que empezará a regir en Octubre de 2004: El inciso 2º pasa a ser párrafo 2. y se le agrega un segundo inciso que establece: *"Igualmente incurrirán en las mismas penas los que importen intencionadamente estos productos sin dicha autorización, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando ellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento".* Al inciso 3º, que pasa a ser párrafo tercero se le agrega al final después de programas de ordenador *o cualquiera de las obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.*

[7] Modificado, Ley Orgánica 15/2003, en vigencia desde octubre 2004 como sigue: letra b) *Que los hechos revistan especial gravedad atendiendo el valor de los objetos producidos ilícitamente o a la especial importancia de los perjuicios causados. c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual. d) Que se utilice a menores de 18 años para cometer estos delitos".*

con el delito cometido, por un período de dos a cinco años, cuando concurre alguna de las siguientes circunstancias:
a) Que el beneficio obtenido posea especial trascendencia económica.
b) Que el daño causado revista especial gravedad.
En tales casos, el Juez o Tribunal podrá, asimismo, decretar el cierre temporal o definitivo de la industria o establecimiento del condenado. El cierre temporal no podrá exceder de cinco años".

Se sancionan las siguientes conductas: la reproducción, el plagio, la distribución, la comunicación pública, importación, exportación o almacenamiento de copias ilícitas.

El plagio no está integrado necesariamente por las versiones sucesivas del programa ni por los programas derivados, que son objeto específico de protección a favor de quien las realice en la Ley de Propiedad Intelectual, que en su artículo 100.4 dispone que el autor, salvo pacto en contrario, no podrá oponerse a que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa o de programas derivados del mismo. La transformación comprende (Art. 99.4 LPI) la traducción, adaptación, arreglo, que forman parte de los derechos de explotación exclusivos que corresponden al titular de los mismos, por lo que quienes la realicen deberán contar con la autorización de éste. Cuando así suceda, la protección se extiende a la transformación. No necesitarán autorización del titular, salvo disposición contractual en contrario, la reproducción o transformación de un programa de ordenador, incluida la corrección de errores, cuando esos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a la finalidad propuesta (Art. 100.1 LPI).

Ahora bien, en cuanto a la reproducción, hay que señalar que dentro de los derechos exclusivos de explotación del programa que corresponden al autor o a quien los haya adquirido se comprende la cesión del derecho de uso, mediante el cual se autoriza a otro a usar el programa, conservando el cedente la propiedad del mismo (Art. 99 LPI.). Se presume, salvo prueba en contrario, que la cesión no es exclusiva, pero sí intransferible y para satisfacer únicamente las necesidades del usuario y que la reproducción total o parcial, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria, deberá contar con la autorización del titular de los derechos de explotación. Cuando la carga, presentación,

ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización del titular. (art. 99.a) LPI).

Esta regla tiene dos excepciones: la del Art. 100.1 LPI, esto es, cuando la reproducción resulte necesaria para la utilización del programa por parte del usuario legítimo, con arreglo a su finalidad propuesta, salvo pacto contrario, y la del Art. 100.3 LPI que se refiere a la realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa, la que no podrá impedirse por contrato, cuando resulte necesaria para la utilización del sistema.

Por lo tanto, fuera de estos casos, la copia, la instalación de cualquier programa de ordenador sin consentimiento del titular del derecho, cae dentro del concepto de reproducción sancionado en esta norma. En principio podría resultar ser constitutiva de delito la copia no autorizada, la cesión onerosa o gratuita a tercero, la instalación más allá de las posibilidades cubiertas por la licencia de uso, etc., incluso si se produce en el ámbito doméstico y para uso privado, circunstancias éstas previstas expresamente en la LPI como infracción al derecho de autor.

Ahora bien, de acuerdo con el artículo 270 del Código Penal, para que la reproducción –y las demás conductas sancionadas– sea constitutiva de delito es necesario que se realice "con ánimo de lucro y perjuicio de tercero". El Tribunal Supremo español, ha definido ánimo de lucro como todo beneficio, ventaja o utilidad patrimonial que pretende obtener el sujeto con la conducta para sí o para tercero, incluso las meramente lúdicas, contemplativas o de ulterior beneficencia.

En cuanto a "en perjuicio de tercero", el sentido del tipo y la referencia conjunta al lucro y al perjuicio señalan que: 1) son conceptos que deben interpretarse en términos patrimoniales y económicos; 2) el tipo considera que ambas exigencias son compatibles y separables, ya que la finalidad de obtener un beneficio económico con la conducta no se traduce necesariamente en el propósito de perjudicar al sujeto pasivo; 3) la acumulación de ambos pretende limitar el ámbito de aplicación del tipo, que resulta más restringido que

cuando se requiere sólo uno de ellos. Según la doctrina, la expresión "en perjuicio" puede entenderse de tres formas: 1) como exigencia efectiva de que como consecuencia de la conducta se cause un perjuicio en el patrimonio ajeno, lo que lo convertiría en el resultado del delito; 2) como elemento subjetivo del injusto, que expresaría una finalidad específica en la conducta de necesaria concurrencia para que el hecho resulte típico; 3) como una característica objetiva del comportamiento, en el cual éste debe resultar objetivamente idóneo (por el número de copias, por el precio, etc.) para causar un perjuicio ajeno, elemento que sólo haría típicos los que tuvieran esa capacidad potencial, esto es, el dolo del sujeto activo.

La última interpretación es la más aceptada, lo que significa que no sería típica por falta de esa capacidad potencial, la infracción que se produzca por el mero uso privado de la misma persona que la realice.

b. Adquisición o recibimiento de copias no autorizadas de programas de ordenador

El artículo 298, ubicado en el Capítulo XIV "*De la recepción y otras conductas afines*", dispone:

> *"1. El que, con ánimo de lucro y con conocimiento de la comisión de un delito contra el patrimonio o el orden socioeconómico, en el que no haya intervenido ni como autor ni como cómplice, ayuda a los responsables a aprovecharse de los efectos del mismo, o reciba, adquiera u oculte tales efectos, será castigado con la pena de prisión de seis meses a dos años.*
> *2. Esta pena se impondrá en su mitad superior a quien reciba, adquiera u oculte los defectos del delito para traficar con ellos. Si el tráfico se realizase utilizando un establecimiento o local comercial o industrial, se impondrá, además, la pena de multa de doce a veinticuatro meses. En estos casos los Jueces o Tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria, por tiempo de dos a cinco años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años.*
> *3. En ningún caso podrá imponerse pena privativa de libertad que exceda de la señalada al delito encubierto. Si éste estuviese castigado con pena de otra naturaleza, la pena privativa de libertad será sustituida por la de multa de seis a veinticuatro meses, salvo que el delito encubierto tenga asignada pena igual a ésta; en tal caso se impondrá al culpable la pena de aquel delito en su mitad inferior".*

El Art. 298 recoge dos modalidades de conducta: 1) ayudar con ánimo de lucro y a sabiendas a los responsables a aprovecharse de los efectos del delito, 2) recibir, adquirir, u ocultar, a sabiendas y con ánimo de lucro las reproducciones ilícitas de los programas.

La adquisición es punible tanto si es gratuita como si se produce mediante precio, cualquiera que sea éste, incluso si es superior al del mercado. La recepción parece referirse a la entrega gratuita de los efectos. La ocultación, equivale a esconderlos, aunque siguen siendo de quien los entregó. Estas conductas constituyen el aprovechamiento propio que se ha considerado siempre característico de la receptación y en el que se incluye cualquier beneficio, ventaja o utilidad patrimonial que obtenga o se proponga obtener el presunto receptador de los efectos del delito previo, incluso los meramente lúdicos, contemplativos, o de ulterior beneficencia.

Sujeto activo sólo puede ser quien no haya intervenido ni como autor ni cómplice en el delito contra el patrimonio o en contra el orden económico del que provienen los efectos. Los "efectos del delito" de los que se beneficia el sujeto son los que integran el objeto material del atentado patrimonial o socioeconómico previo, en este caso, las copias ilícitas de los programas de ordenador.

El "conocimiento de la comisión de un delito", de la naturaleza ya señalada, elemento del dolo, significa el conocimiento de que la copia que se adquiere, recibe u oculta proviene de un delito, lo que se ha interpretado como certeza y no como simple sospecha. No es necesario que el sujeto conozca ni la calificación jurídica exacta del delito previo, ni las circunstancias en que se produjo. No es necesario conocer a los autores y partícipes del delito del que provienen los efectos, ni que el delito principal haya sido castigado.

El ánimo de lucro se considera presente en quien recibe o adquiere una copia pirata de un programa, la existencia de la receptación dependerá de su integración a un delito contra la propiedad intelectual. Cuando al sujeto le conste que la copia proviene de una reproducción ilícita con incidencia en el mercado, su comportamiento podrá calificarse de receptación. El

conocimiento se dará por sentado en quien adquiera la copia en ciertas condiciones (ofertas con un valor muy inferior al real, inexistencia de manuales o licencias de uso, etc).

c. Conductas relacionadas con la desprotección de programas de ordenador

El párrafo tercero del Art. 270 considera como delito la fabricación, puesta en circulación, incluso gratuita, o la tenencia de medios físicos o lógicos (copiones) específicamente dirigidos a desproteger programas de ordenador, con el fin de poder efectuar reproducciones, instalaciones o copias no autorizadas de los mismos. Se exige que el medio sirva "específicamente" para esta finalidad, de este modo se limita drásticamente la aplicación de la norma, que no sería invocable, por ejemplo, respecto de medios que junto a la posibilidad de desproteger programas, incluyan utilidades distintas (comprensión/descomprensión de ficheros, encriptación/desencriptación, etc.).

La conducta típica incluye la fabricación, puesta en circulación y tenencia de tales programas o dispositivos. No requiere ánimo de lucro ni perjuicio de tercero, por lo tanto, puede resultar constitutiva de delito la mera tenencia de los mismos por cualquier usuario que los emplea exclusivamente para uso privado. Pareciera que la disposición viene a castigar simples actos preparatorios, lo que en relación con la mera tenencia llevaría demasiado lejos la intervención penal.

3.1.4 Utilización Ilegítima de Terminales de Comunicación.

Artículo 255. *"Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido 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".

Artículo 256. *"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".*

La Ley General de Telecomunicaciones de 1998, entiende por equipo terminal: "*equipo destinado a ser conectado a una red pública de telecomunicaciones, esto es, a estar conectado directamente a los puntos de terminación de aquélla o interfuncionar, a su través, con el objeto de enviar, procesar o recibir información".*

La mención de las "telecomunicaciones" permite incluir las defraudaciones en el teléfono, la televisión por cable o de pago, la transmisión de datos –analógica o digital–, el acceso a bancos de datos, etc., siempre que tales servicios se suministren mediante redes o instalaciones distribuidoras y se tarifen mediante aparatos contadores o instrumentos específicos de recepción y fijación del consumo, cualquiera que sea su clase o configuración técnica. Lo que se sanciona es el uso en beneficio propio y en perjuicio del suministrador de este tipo de energías o fluidos cuando se hace con comportamientos que afecten directamente a la red de distribución o prestación del servicio o a los mecanismos o verificaciones precisas para la determinación del consumo efectuado. No comprende, los supuestos de utilización ilegítima de sistemas informáticos que funcionan con las energías o acceden a los servicios defraudados, que sólo resultan punibles en los términos del artículo 256 (multa de tres a doce meses). En concreto, lo que el artículo 255 sanciona son las defraudaciones realizadas por el titular del sistema informático (o por su orden) en perjuicio de quien le suministra el servicio, mientras que los casos genuinos de utilización ilegítima de equipos son las que se producen en perjuicio del propietario de los mismos por quienes están encargados de su manejo. Las telecomunicaciones defraudadas deben tener un valor superior a cincuenta mil pesetas (400 euros a partir de octubre de 2004), si fuera inferior constituirá falta.

Las defraudaciones que se producen como consecuencia de la indebida utilización de terminales de telecomunicaciones, sin consentimiento de su titular, cuando se causa un perjuicio superior a cincuenta mil pesetas, se castigan en el Art. 256. Si el perjuicio fuera inferior constituye falta. Terminales de telecomunicaciones son todos los que, cualquiera que sean sus características concretas, sirven para establecer conexiones a distancia entre personas, sistemas o dispositivos técnicos, mediante procedimientos eléctricos, radioeléctricos, informáticos, telefónicos etc. El uso no autorizado puede consistir en la utilización del terminal ajeno sin consentimiento del dueño o en su empleo en tareas o con finalidades

distintas de las permitidas. Dentro de la disposición quedan comprendidas determinadas formas de hacking, como el acceso ilícito mediante un ordenador propio a redes o sistemas informáticos ajenos, utilizando recursos o programas instalados en el mismo.

Es necesario hacer presente que sólo se sanciona la utilización de equipos informáticos cuando éstos cumplen funciones de terminales de telecomunicación, pero no cuando sirven simplemente para el procesamiento de información de manera autónoma. No está incluida la indebida utilización de ordenadores conectados en una red local, unidos directamente entre sí e integrados en un conjunto de equipos de funcionamiento independiente. En los casos que no exista la dimensión externa, el hecho sólo podrá ser considerado un ilícito civil (o laboral).

Gran parte de la doctrina ha sostenido que en este caso el legislador se ha extralimitado, no respetando el principio de intervención mínima que preside el Derecho penal, criminalizando un supuesto cuya solución conflictual y adecuada tutela de los derechos del tutelar del equipo no debe trascender la vía civil, por vía de la reparación, en el caso de los particulares, o la vía de la sanción administrativa, en el caso de equipos pertenecientes a la Administración Pública y tratarse de funcionarios públicos que abusaren de los mismos.

Corresponde tratar a continuación los ilícitos patrimoniales que se realizan sirviéndose de los sistemas informáticos o de sus elementos, que aparecen como instrumento necesario para la realización de la correspondiente conducta típica.

3.1.5 Los Ilícitos patrimoniales realizados por medio del sistema informático:

a. Estafa por medios informáticos.

> Artículo 248[8]. *"1. Cometen estafa los que, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*

[8] La reforma introducida por la Ley Orgánica 15/2003, le añadió un apartado 3: "*La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo".*

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

A través de la referencia "alguna manipulación informática o artificio semejante" se pretende incorporar todos los casos posibles mediante los que se efectúa una transferencia no consentida de activos patrimoniales en perjuicio de un tercero, tanto las modificaciones de programas o alteraciones en el procesamiento como las manipulaciones de entrada, salida o transmisión de datos. La referencia a "o artificio semejante" podría hacer pensar que incluye otras maniobras de naturaleza no informática, sin embargo, el sentido del apartado obliga a entender que todo él va referido a estos supuestos, por lo que la mención legal debe ser interpretada desde esa perspectiva.

En cuanto a los elementos del delito, estos son semejantes a los de la estafa: ánimo de lucro; la manipulación informática o artificio semejante, equivale al engaño bastante y al error; la transferencia no consentida es el acto de disposición que causa el perjuicio al tercero; se precisa la relación causal entre la manipulación informática, la transferencia electrónica y el perjuicio ajeno. En la práctica, la transferencia se hará directamente por el sistema informático que reciba la orden fraudulenta, de manera que la mención a "no consentida" no se entiende como la existencia de un acto concreto de voluntad contrario a la transferencia, que no existirá, sino como una orden de cargo hecha en activos patrimoniales ajenos sin derecho a ello.

La disposición sanciona sólo las transferencias electrónicas de fondos, no comprende las conductas que no provoquen una operación de este tipo, por lo tanto no se incluyen –sino en la modalidad delictiva que corresponda en cada caso–, las manipulaciones cuyo objetivo sea apoderamientos o disposiciones efectuadas por otros medios (ejemplo, alterar la contabilidad para encubrir desfalcos, etc.). Transferir (cambiar de un lugar a otro), en el texto, es un proceso meramente contable que supone cargar débitos, descontar activos u ordenar ingresos con la correlativa anotación a favor de otro sujeto, al que de esta forma se le reconoce un derecho a crédito o a favor del que se realiza una cierta prestación o servicio. La

consumación se produce cuando se realiza el perjuicio, lo que coincidirá con la realización del asiento contable. La tentativa es posible.

b. Apoderamiento de dinero utilizando tarjetas de créditos.

Para la doctrina española, el uso indebido de tarjetas de crédito con la finalidad de obtener dinero en efectivo desde cajeros automáticos es equiparable al de las maniobras físicas sobre máquinas automáticas cabinas telefónicas, expendedoras de tabaco, cigarrillos, etc.), cuando se persigue obtener de ellas el producto o el servicio sin la correspondiente contraprestación económica. Estos casos deben ser considerados como hurto cuando lo que se obtiene es una cosa mueble. Hay objeto material, dado que lo que se obtiene es dinero y no un asiento contable. La posibilidad de estafa debe ser descartada puesto que no hay engaño a "otro", como requiere el tipo básico del 248.1 ni se trata de una transferencia no consentida de activos patrimoniales, como lo exige el 248.2, sino directamente de la obtención de dinero que puede ser considerado cosa mueble.

c. Abuso de Cajeros Automáticos.

Para González Rus, cuando lo que se produce son extracciones repetidas por el titular, superando el saldo disponible, no se puede hablar de apoderamiento de cosa mueble ajena ya que falta la ajenidad del dinero recibido y la ausencia de consentimiento del propietario de la cosa, puesto que el contrato de depósito en cuenta corriente o de apertura de crédito que vincula a la entidad y al usuario de la tarjeta genera entre ellos derechos de créditos recíprocos y acepta la posibilidad de descubiertos, lo que podría considerarse un consentimiento tácito sobre la obtención del dinero por cuantía superior a la existente en el momento de realizar la extracción; esto sin mencionar la posibilidad de que se pueda suponer un comportamiento atípico como consecuencia de la aceptación del riesgo que supone la delegación en el usuario de funciones de autoprotección que corresponden a la entidad emisora. Por lo tanto, podría ser considerado un mero ilícito civil, esto es, una falta.

Para el mismo autor, en el supuesto en el que el titular utiliza una tarjeta anulada o caducada, se estaría ante un caso de utilización de la tarjeta por un tercero sin derecho a ello. Al no haber contrato vigente entre la entidad bancaria y el titular, se aprecia un hurto por la cantidad que se obtenga. La retención de la tarjeta por el cajero al constatar la anomalía, dará lugar a la tentativa.

Agrega, que en los casos en que la extracción de dinero se produce por un tercero con tarjeta falsificada, perdida o sustraída al titular, hay que distinguir: si la tarjeta fue encontrada y no devuelta se trataría de una apropiación indebida; si fue sustraída, un hurto, si se obtuvo mediante engaño, una estafa; en los tres casos, por el importe de la tarjeta en sí, lo que significaría apreciar una falta. Sujeto pasivo de estas infracciones será el propietario de la tarjeta, que normalmente es la entidad emisora. Cuando se la quiere para utilizarla y devolverla después, se realizarían esas infracciones en su modalidad de uso, que son atípicas. La obtención del número de identificación personal mediante engaño no constituye estafa respecto de lo que después se obtiene con la tarjeta, porque en estos casos en los que se "engaña" al cajero, la figura aplicable es hurto y no estafa. Respecto del dinero que se extraiga el apoderamiento de la tarjeta no es acto de ejecución, por lo que la sustracción sólo será punible en cuanto tal, sin constituir además la tentativa de robo.

Algunos tratadistas consideran que no es posible la aplicación del hurto cuando el cajero automático se utiliza de forma "técnicamente correcta" por un no autorizado y que sólo habría delito cuando la obtención se produce en forma "anormal". El primer caso ocurre cuando el Banco, una vez conocida la pérdida o la sustracción de la tarjeta, no ha adoptado las medidas necesarias para invalidar o bloquear la tarjeta, pues sólo dichas medidas acreditan su voluntad manifiesta de que la misma no sea utilizada. Argumentan que el cajero hace lo que su programa establece y que el Banco establece el programa que quiere, es decir lo que su dueño quiere que haga, y dado que tal programa hace que el cajero entregue dinero a quien disponga de la tarjeta y el número clave, el Banco asume voluntariamente el riesgo de que personas no autorizadas obtengan el dinero.

Para González Rus el dinero que se obtiene del cajero automático con tarjeta ajena, dará lugar a un hurto –dejando a salvo lo dispuesto en el artículo 239, párrafo 2º, que se refiere al robo con fuerza en las cosas–. Ahora la determinación de quién es sujeto pasivo y quién perjudicado dependerá de las cláusulas contractuales que se hayan establecido en los casos de pérdida o sustracción y las obligaciones y responsabilidades que asuma el titular por una parte, y la entidad emisora por la otra. La simple utilización de la tarjeta supone la realización de actos de ejecución, de manera que si por causas ajenas a la voluntad del sujeto, no se obtiene el dinero, constituirá tentativa. De ser punible la apropiación de la tarjeta, dará lugar a concurso medial (ideal) de delitos.

d. Utilización de Tarjetas de Cajeros Automáticos y Fuerza en las Cosas.

El artículo 239.2 ubicado en el Capítulo "De los robos", dispone:

"Se considerarán llaves falsas:

.../...

2º Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
A los efectos del presente Artículo, se consideraran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia".

En consecuencia, la tarjeta utilizada para abrir el habitáculo en el que se encuentra el cajero automático debe ser falsa. Esta consideración tienen las señaladas en el número 2º. Sin embargo, si la tarjeta se utiliza para obtener directamente el dinero del cajero, no se puede decir que sirva para abrir un cierre, sino que se desencadena un proceso mecánico en virtud del cual se produce la entrega automática del dinero, no cumple realmente la función de llave. En este caso un sector doctrinal dudó que pudiera considerarse un robo, otro, en cambio, no encontró dificultades para estimarlo. La discusión fue zanjada por la Fiscalía General del Estado, que en Consulta 2/1988, lo consideró como delito de robo con fuerza en las cosas, por uso de llave falsa.

3.1.6 Infracciones a la Intimidad y Privacidad.

Artículo 197. *"1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apoderare de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otro documento o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen, o de cualquiera otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos de un tercero.
3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.
5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o incapaz, se impondrán las penas previstas en su mitad superior.
6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años".

Ahora bien, el apartado 1, inciso primero, se refiere al delito de apoderamiento de secretos documentales personales, figura clásica en la que se introducen dos situaciones vinculadas con los medios informáticos y las nuevas tecnologías de telecomunicación: la primera, protege una amplia gama de soportes que contengan secretos de una persona de acuerdo con el concepto de documento establecido en el artículo 26[9] del Código Penal; la segunda, incorpora expresamente los mensajes de correo electrónico como objetos sobre los cuales puede recaer la acción de apoderamiento por parte del sujeto activo. Lo más importante

[9] Artículo 26. *"A los efectos de este código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".*

y determinante de la disposición es el específico elemento subjetivo del injusto constituido por la finalidad de descubrir los secretos o vulnerar la intimidad de otro.

El apartado 1, inciso 2º, se refiere al delito de interceptación para descubrir secretos personales o vulnerar la intimidad de otro, si bien parte de la doctrina lo denomina "Intrusismo con interceptación" considerando que de acuerdo con la cláusula abierta de "cualquier otra señal de comunicación", se amplia el ámbito de la tutela penal a futuras innovaciones tecnológicas de comunicaciones telemáticas, no es menos cierto que en el Anexo de la Ley General de Telecomunicaciones se mantiene un concepto muy amplio y generoso de lo que se entiende por telecomunicaciones, como *"toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos y otros sistemas electromagnéticos"*. Se entiende consumado cuando se efectúa la interceptación o la utilización de los artificios técnicos, por lo tanto constituye un delito de mera actividad, siendo entonces factible que la información secreta o relativa a la intimidad esté representada por datos informáticos y sea transmitida por vía telemática o de telecomunicación, siendo éstas vías el objeto sobre el que recae la acción, pero sin necesidad de un efectivo descubrimiento de la intimidad, aparece también como bien jurídico protegido la seguridad de las vías de transferencia de datos.

El apartado 2 se refiere al delito de vulneración del habeas data, tipificando un abanico de diversas conductas ilícitas contra la privacidad, informáticas o no, desde el apoderamiento, utilización, modificación, no autorizados y en perjuicio de tercero de datos personales y familiares, hasta el mero acceso no autorizado a los mismos, o su alteración o utilización, no autorizados, en perjuicio del titular de los datos o de un tercero. Lo más importante es la previsión que se efectúa como sancionable del "*mero acceso no autorizado de los datos personales y familiares*", cuando los mismos se encuentran en un archivo informático o automatizado, lo que pudiera comprender el *hacking* informático, posibilidad ésta que queda desvirtuada cuando se exige que se cause un "*perjuicio del titular de los datos o de un tercero*" tanto respecto de las acciones de alterar o utilizar como a la acceder, lo que podría ser solventado si existiera una coma antes de la conjunción "y" que une las acciones de "*acceda por cualquier medio a los mismos*" con "*a quien los altere o utilice*".

Por su parte, el artículo 200 dispone: "*Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código*". Con esta disposición se establece la posibilidad de protección de las personas jurídicas como sujetos pasivos de estos ilícitos, cuando en realidad el bien jurídico protegido debe ser la intimidad de las personas individuales.

3.2 FRANCIA.

Con la Ley de Modificación del Código Penal, número 88-19, de 5 de enero de 1988, relativa al fraude informático, también conocida como "*loi Godfrain*", el legislador recogió en un nuevo Capítulo del Código Penal, bajo la rúbrica "Sobre ciertas infracciones en materia informática" (especialmente los delitos vinculados a la piratería, intrusión, traba al funcionamiento, esto es virus y ciertas asociaciones que pueden ser de hackers) toda la nueva realidad criminal compleja vinculada a las nuevas tecnologías de la información, pero siempre y cuando no tuvieran ya una adecuada inclusión bajo figuras clásicas existentes. En este sentido, la utilización frecuente del término "informatisé" (informatizado) sobre el de "informatique" (informático), ha hecho pensar a la doctrina que el legislador se ha preocupado de proteger la información en su conjunto y no sólo aquella en soporte informático, es decir, que su preocupación se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas con ánimo de lucro y en perjuicio patrimonial de tercero, núcleo principal del fraude informático.

Es así como, el título genérico de la ley hace referencia al fraude informático, en el enunciado, en su texto no aparece ninguna referencia específica al mismo. Es más, la ley sanciona específicamente la falsedad informática, sólo cuando el dato alterado se encuentre sobre un soporte informático.

Por lo tanto, las defraudaciones patrimoniales por medios informáticos quedan sin regulación especial, porque de acuerdo con las decisiones y jurisprudencia de la Corte de

Casación Francesa y de los Tribunales de Apelación, aquellas venían siempre subsumidas en la figura clásica de estafa del Art. 405 del Código Penal, que sanciona al que "*haciendo uso de falsos nombres o de falsas cualidades, bien empleando maniobras fraudulentas para simular la existencia de falsas empresas, de un poder o crédito imaginario, o por hacer nacer la esperanza o la creencia de un suceso, de un accidente o de cualquier otro acontecimiento imaginario, se haya hecho reintegrar o traspasar, o hubiera intentado hacerse reintegrar o traspasar fondos, muebles, obligaciones, disposiciones, billetes, promesas, deducciones o desgravaciones, y hubiera por uno de estos medios, defraudado o intentado defraudar la totalidad o parte de la fortuna de otro".*

La subsumisión es posible al recogerse en la descripción de la conducta típica la cláusula "maniobras fraudulentas" y el "perjuicio", debiéndose entender éstas como formas de engaño, siendo las manipulaciones informáticas integrables en aquéllas, y la omisión del texto a referencias genéricas sobre el "engaño", el "error" y al "acto de disposición". Al respecto, según la doctrina, la ley de reforma francesa se concibe materialmente como una vía para reprimir accesos abusivos a los sistemas informáticos y actuaciones ilícitas sobre datos informatizados y su tratamiento, se produzca o no perjuicio, habiéndose rechazado de forma expresa en el proceso de tramitación parlamentaria las propuestas de subsumir las agresiones patrimoniales por medios informáticos en los tipos recogidos por esta ley.

La reforma penal de 1992, Ley 92-683, vigente a partir de marzo de 1994, introdujo cambios en el texto legal de las disposiciones informáticas y las trasladó a otra parte del Código, esto es, al Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos. La falsificación informática que estaba regulada en los artículos 462-5 y 462-6, sobre la falsificación y uso de documentos electrónicos falsificados, actualmente en el nuevo Art. 441-1, que se refiere a todas las posibles formas de un documento, incluyendo el electrónico. El acceso fraudulento en sistemas informáticos en el actual 323-1, sabotaje informático en el artículo 323-2.

3.2.1 Acceso fraudulento a un sistema de elaboración de datos.

> Artículo 323-1. "*El hecho de acceder en forma fraudulenta a la totalidad o parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él, será castigado con un año de prisión y multa de 15.000 euros.*
> *Si de ello resultare, bien la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento de este sistema, la pena será de dos años de prisión y de 30.000 euros de multa".*

Para que se entienda consumado este delito, no se requiere la alteración, daño o destrucción de los datos contenidos en el sistema, ni el apoderamiento, uso o conocimiento de la información contenida en él, y tampoco la revelación o difusión de los datos contenidos en ese sistema. La mención a "mantenerse en él", se refiere al acceso que ocurre en forma accidental o casual.

3.2.2 Sabotaje informático

> Artículo 323-2. *"El hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos será castigado con tres años de prisión y multa de 45.000 euros".*

La legislación francesa, al igual que la alemana distingue entre el delito de sabotaje informático y la alteración de datos.

3.2.3 Destrucción de datos.

> Artículo 323-3. *"El hecho de introducir de manera fraudulenta datos en un sistema de tratamiento automatizado o de suprimir o modificar fraudulentamente los datos que contengan será castigado con tres años de prisión y multa de 45.000 euros".*

El objeto del delito son los datos contenidos en un sistema de tratamiento de los mismos.

3.2.4 Asociaciones para cometer delitos informáticos.

Artículo 323-4. *"La participación en un grupo formado o en un acuerdo establecido para la preparación, caracterizada por uno o varios hechos materiales, de una o varias de las infracciones previstas en los artículos 323-1 a 323-3 será castigada con las penas previstas para la misma infracción o para la infracción castigada más severamente".*

Se trata de los llamados Clubs de Hackers.

Artículo 323-5. *"Las personas físicas culpables de los delitos previstos en el presente capítulo incurrirán igualmente en las penas accesorias siguientes:*
1º La prohibición, por un período hasta de cinco años, del ejercicio de derechos cívicos, civiles y de familia, según las modalidades del artículo 131-26;
2º La prohibición, por un período de hasta cinco años, de ejercer una función pública o de ejercer la actividad profesional o social en el ejercicio de la cual o con ocasión de la cual se haya cometido la infracción;
3º El comiso de la cosa que haya servido o estaba destinada a cometer la infracción o de la cosa producto de la misma, con excepción de los objetos susceptibles de restitución;
4º La clausura, por un período de hasta cinco años, de los establecimientos o de uno o varios de los establecimientos de la empresa que hayan servido para cometer los hechos incriminados;
5º La exclusión, por un período de hasta cinco años de los contratos públicos;
6º La prohibición, por un período de hasta cinco años, de emitir cheques, salvo los que permitan la retirada de fondos por el librador contra el librado o los que estén conformados;
7º La publicación o la difusión de la resolución adoptada en las condiciones previstas en el artículo 131-35".

Artículo 323-6. *"Las personas jurídicas podrán ser declaradas penalmente responsables de las infracciones definidas en el presente capítulo en las condiciones previstas en el artículo 121-2.*
Las penas aplicables a las personas jurídicas serán:
1º La multa, conforme a lo previsto en el artículo 131-38;
2º Las penas mencionadas en el artículo 131-39.
La prohibición mencionadas en el apartado 2º del artículo 131-39 se aplicará a la actividad en cuyo ejercicio o con ocasión de la cual se haya cometido la infracción".

Artículo 323-7. *"La tentativa de los delitos previstos en los artículos 323-1 a 323-3 será castigada con las mismas penas".*

3.2.5 Falsificación y uso de documentos electrónicos falsificados.

> Artículo 441-1. *"Constituye una falsedad toda alteración fraudulenta de la verdad, susceptible de causar un perjuicio y realizada por cualquier medio, en un escrito o en cualquier otro medio de expresión de pensamiento que tenga por objeto o que pueda tener como efecto constituir la prueba de un hecho con consecuencias jurídicas o de un derecho".*

El legislador francés suprimió los artículos 462-5 y 462-6, sobre falsificación y uso de documento electrónico falsificado, y amplió el concepto de documento de manera de incluir los electrónicos.

3.3 ALEMANIA.

La reforma penal en materia de delitos informáticos, vino como consecuencia de la insuficiencia y deficiencias de las normas tradicionales y los tipos clásicos en ellas previstas. Un largo debate, iniciado a mediados de la década de los setenta, dio como resultado la "Segunda Ley de Lucha contra la Criminalidad Económica" de 1986.

Las modificaciones introducidas por esta Ley en el Código Penal Alemán, respecto de las conductas delictuales relacionadas con los medios informáticos, no sólo consistieron en la modificación de alguna disposición ya existente, sino que en algunos casos se introdujeron nuevas figuras o tipos penales.

Entre las nuevas figuras que regula Ley se encuentran: el espionaje de datos (párrafo 202.a), estafa mediante ordenador o fraude informático (párrafo 263.a), falsificación de datos probatorios (párrafo 269), modificaciones complementarias del resto de las falsedades documentales (párrafo 270, 271, 273, 274 y 348), engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (párrafo 270), modificación de datos (párrafo 303.a) y sabotaje informático (párrafo 303.b).

3.3.1 Espionaje de datos.

> Párrafo 202.a *"I. Quien consiga sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa.*
> *II. Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible".*

El tipo protege el interés formal en el mantenimiento del secreto por parte del titular para disponer del almacenamiento y trasmisión de datos no directamente perceptibles, el que a través de su protección manifiesta su interés en el mantenimiento del secreto.

Sujeto activo sólo puede ser aquel para el cual no están previstos los datos, de manera que no contempla el supuesto del empleado que sin autorización utiliza datos para el accesibles. La punibilidad está limitada a los datos que están especialmente protegidos contra el acceso no autorizado (ejemplos, contenedores cerrados, contraseñas, encriptados, etc.).

Del concepto de datos del inciso segundo del párrafo 202.a, se desprende que es necesario que el acto de espionaje recaiga sobre datos no perceptibles directamente.

3.3.2 Estafa informática.

> Párrafo 263.a *"I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.*
> *II. Procede aplicar el 263, apartados II a V.*

El párrafo 263.a contempla la conceptuación de la figura como tipo básico en el inciso primero, y la sanción de la forma imperfecta de ejecución (tentativa) y un supuesto de agravación del tipo en razón de la gravedad del hecho (privación de libertad de uno a 10 años) por la remisión que efectúa al párrafo 263.

Se prescinde de la conceptuación restrictiva de los elementos clásicos de la estafa[10] que dificultan la aplicación de ésta a las defraudaciones cometidas mediante ordenador: el engaño a una persona (mención que no aparece en la estructura del tipo), el error en la misma (desaparece asimismo el requisito de provocación o mantenimiento del error en tercero), y el acto de disposición patrimonial lesivo (que en el caso de concurrir puede ser ya realizado tanto por una persona como por el propio ordenador automáticamente), requiriéndose en su lugar sólo al resultado de un perjuicio patrimonial para otro. Permanecen los elementos subjetivos, especialmente el de la intención de conseguir una ventaja patrimonial, y los medios comisivos de influencia en el desarrollo del resultado de un proceso de transformación de datos se establecen alternativamente a través de la configuración errónea del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso.

El proyecto del gobierno entendió por "proceso de datos" todos aquellos procesos técnicos en los que se alcanzan determinadas conclusiones de trabajo a partir de la toma de datos y de su puesta en relación según determinados programas. Se contempla aquí únicamente el proceso automático de datos. Según las reglas alemanas un programa es una instrucción completa para la resolución de una tarea junto con todos los ajustes precisos para ello, los programas informáticos son instrucciones de trabajo para el ordenador.

La configuración incorrecta, es la modificación del programa para que sus instrucciones sean distintas a las concebidas inicialmente por su propietario: introducción de nuevas instrucciones o funciones en el programa, eliminación o alteración de su proceso de funcionamiento, modificación de los sistemas de control del propio programa, etc. El criterio para determinar la incorrección del programa es la intención del usuario del mismo, el hecho que éste lo haya aprobado por desconocimiento de la incorrecta configuración no exime de responsabilidad al sujeto activo del delito.

[10] El párrafo 263 I. Se refiere a la estafa en los siguientes términos *"Quién, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro causando un error o manteniéndolo, por medio de la apariencia de hechos falsos o de la desfiguración o supresión de hechos verdaderos, será castigado con pena de privación de libertad de hasta cinco años y con multa".*

En cuanto a la situación que se refiere al empleo de datos incorrectos o incompletos comprende la manipulación en el *input* o entradas, no sólo por el operador o usuario del terminal que suministra de modo inmediato datos falsos a la instalación del proceso electrónico de datos, sino también por quienes los proporcionan de modo inmediato, como el personal de clasificación de datos (perforadores, mecanógrafos, etc.). Se incluyen los casos de determinación a través de terceros ajenos (ej. clasificación de datos primarios), como los casos de suministro inmediato, en que intercalan terceros que no practican ninguna comprobación material de los datos.

De acuerdo con la doctrina alemana, el que utiliza una tarjeta falsificada de acceso al ordenador emplea datos incorrectos del mismo modo de quien falsifica estados de cuenta.

En cuanto a la influencia en el resultado de un proceso de elaboración de datos a través de un uso no autorizado de datos, la doctrina alemana, considera que de este modo se ha cubierto el supuesto del que mediante uso ilegítimo de tarjeta (las de cajero) y de códigos ajenos consiga acceder a sistemas informáticos con efectos patrimoniales de relevancia.

Respecto de la influencia en el resultado de un proceso de elaboración de datos a través de intervención no autorizada en el proceso, la misma doctrina, la considera una fórmula amplia que pretende evitar posibles lagunas legales, abarcando supuestos no subsumibles en las alternativas anteriores, o de dudosa subsunción.

Ahora bien, al no recoger expresamente, la fórmula alemana, el término ordenador o informático tienen cabida en el precepto las manipulaciones fraudulentas de tipo patrimonial sobre cualquier tipo de sistemas automatizado de toma de decisiones, y no únicamente informático, consistiendo la acción típica en interferir en el resultado de un proceso de tratamiento de datos, de lo que se deriva una interferencia en una disposición patrimonial.

3.3.3 Falsificación de datos probatorios.

> Párrafo 269. *I. Quien, para engañar en el tráfico jurídico, almacene o altere datos probatorios relevantes de manera que en el momento de su recepción existiría un documento no auténtico o falsificado, o utilice datos almacenados o alterados de ese modo será castigado con pena de privación de libertad de hasta cinco años o con multa.*
> *II. La tentativa es punible.*
> *Deberá aplicarse el ξ 267, apartado III".*

La doctrina alemana, ha señalado que en ese país, el tipo de falsedad documental no es aplicable a la llamada falsificación de datos probatorios, debido a la imposibilidad de percibir directamente la declaración y la identidad del otorgante.

La acción consiste en modificar datos ya almacenados o almacenar otros nuevos con el mismo fin, o en utilizarlos en esas condiciones. Es necesario que la visualización de los datos sea equiparable a la existencia de un documento no auténtico o falsificado, es decir, que si fueran impresos o transcritos esos datos constituirían falsedad documental al tenor del párrafo 267.

En cuanto a los elementos del tipo subjetivo, además del dolo (basta que sea eventual), debe concurrir la intención de engañar en el tráfico jurídico. Según la doctrina alemana este requisito se cumple cuando el autor sólo quiere producir la manipulación en el proceso de datos, por lo tanto, no se exige el contacto personal entre el autor y la víctima (a diferencia de cómo es interpretado el engaño en el tipo de estafa). El artículo 270 aclara las dudas sobre el contenido de este elemento, con la innovación de equiparar el engaño a las manipulaciones informáticas, al disponer "*La falsificación de una elaboración de datos en el tráfico jurídico equivaldrá al engaño en el tráfico jurídico".* Esta norma es aplicable a todos los tipos legales en los que se exige "el engaño en el tráfico jurídico", teniendo gran importancia al considerar que la manipulación fraudulenta del proceso de datos produce un efecto similar al engaño.

3.2.4 Alteración de datos.

Párrafo 303.a. *"I. Quien borre, elimine, inutilice o altere ilícitamente datos (202.a, apartado II) será castigado con pena de privación de libertad de hasta dos años o con multa*
II. La tentativa será punible".

La disposición protege tanto al que almacena los datos, como a la persona afectada por el contenido de éstos. Objeto de la acción, son todos los datos no inmediatamente perceptibles en el sentido del párrafo 202.a.II. Se mencionan cuatro acciones típicas: a) el borrado, los hace desparecer de modo completo e irrecuperable (Ej. la destrucción de soportes, borrar los enlaces necesarios y perder la interpretabilidad, etc.); b) ocultar, privando del acceso a los mismos a la persona autorizada; c) inutilizar, cuando se dañan de manera tal que no puedan cumplir su fin; d) alterar, se trata de perturbaciones funcionales, como la transformación de su valor informativo, puede tener lugar a través del añadido de datos, el borrado parcial o la puesta en relación con otros datos. Lo decisivo es que los datos posean un nuevo contenido una información alterada.

3.3.5 Sabotaje informático

Párrafo 303b. *"Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,*
1. *cometiendo el hecho de acuerdo al párrafo 303.a.II, o*
2. *destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos,*

será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. la tentativa será punible".

La finalidad perseguida por la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, fue sancionar con mayor severidad las acciones que atentan contra procesos de datos que sean de importancia esencial para una empresa o establecimiento industrial ajenos o para la administración. Estas acciones pueden recaer en los equipos de procesamiento de datos, en los soportes y en los datos mismos. La doctrina entiende que es sancionado penalmente el que arremete a equipos o soportes de datos suyos en los que otras personas tengan un interés jurídicamente protegido o si borra datos que

el mismo hubiera almacenado y que fueran procesados para terceros cuyo interés en su existencia se perjudica.

3.4 ITALIA.

El Código Penal italiano tipifica los siguientes delitos informáticos:

3.4.1 Acceso abusivo a un sistema informático o telemático (artículo 615 tercero)

Se configura exclusivamente en caso de sistemas informáticos o telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso al mismo sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

3.4.2 Difusión de programas dirigidos a producir daños o interrumpir un sistema informático o telemático (artículo 615 quinto)

El que difunda un programa informático que tenga por objeto el daño a un sistema informático o telemático, datos, o programas, o la interrupción total o parcial de funcionamiento puede ser condenado hasta dos años de prisión.

3.4.3 Atentado contra un sistema informático o telemático de utilidad pública (artículo 420)

Se sanciona con pena de prisión a quien dañe o destruya un sistema informático de utilidad pública.

3.4.4 Abuso de la calidad de operador de sistema.

Este delito es una agravante del delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de comisión del delito.

3.4.5 Detentación y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos (Artículo 615 cuarto)

Castiga al que con el fin de obtener para sí o para otro un beneficio o causando un daño a otro, abusivamente se apodera, reproduce, difunde, comunica códigos, palabras claves u otro medio idóneo que permita el acceso a un sistema informático o telemático.

a. Difusión de programas dirigidos a dañar o interrumpir un sistema informático (Artículo 615 quinto).

b. Violación de la correspondencia electrónica (articulo 616)

c. Intercepción abusiva. (Artículo 617, cuarto, quinto)

Está tratado junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. La intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, de todo o parte, por cualquier medio del contenido de la comunicación se castiga con reclusión de seis meses a cuatro años. Se castiga también la instalación de aparatos para interceptar, impedir o interrumpir las comunicaciones informáticas o telemáticas.

3.4.6 Falsificación informática (617 sexto)

Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. Documento informático está definido por la doctrina italiana como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

3.4.7 Espionaje informático.

3.4.8 Fraude informático (Artículo 640 tercero)

La disposición establece que cualquiera que procure un beneficio para sí o para otro alterando de cualquier modo el funcionamiento de un sistema informático, sobre los datos, las informaciones o los programas comete delito de fraude informático. La pena se agrava si el sujeto activo es operador del sistema informático.

3.4.9 Ejercicio arbitrario de la propia razón con violencia sobre programas informáticos (Artículo 392)

Los virus informáticos pueden ser usados como una excelente herramienta para la protección de los derechos intelectuales y los negocios contractuales. Pero estas conductas pueden no ajustarse a Derecho. Si un programador inserta un virus en un programa a fin de que, en caso de copia, el mismo se active y destruya la información existente en el ordenador es posible considerar la situación como abuso de Derecho. Si bien el titular de la obra de software está en su derecho de proteger sus intereses como autor o dueño, dicha facultad no debe extenderse más allá de lo que razonablemente expliciten las leyes, o el contrato que lo relacione con el usuario. El Código Penal italiano en el artículo 392, sanciona el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

IV. CONCLUSIONES.

Con la promulgación del Código Penal de 1995, el legislador español, al introducir aspectos informáticos o vinculados a las nuevas tecnologías de la información, y al incorporar nuevas figuras delictivas, ha seguido los esquemas dogmáticos penales tradicionales, esto es completar las figuras clásicas para que éstas puedan abarcar a la delincuencia informática. Para esto, ha recurrido, generalmente, a la creación de los llamados tipos de equivalencia, como en el caso del artículo 248.2, o modificando o ampliando algunos elementos o requisitos en las figuras delictuales ya existentes, y efectuando la doctrina y la jurisprudencia, en base a ello, la correspondiente subsunción de nuevos comportamientos abusivo informáticos por la vía de la interpretación correctiva de los preceptos clásicos.

En Francia la Ley Nº 88-19, relativa al Fraude Informático, de 1992, introdujo el capítulo II al libro II del título II del Código Penal, bajo la denominación "De ciertas infracciones en materia informática". Esta ley fue modificada por la Ley 92-683 de 1992, que trasladó las disposiciones informáticas al Libro II, Título II, Capítulo III. De los atentados contra los sistemas de tratamiento automatizado de datos.

El legislador francés utilizó la técnica legislativa especial, esto es, la conducta la criminalizó por medio de una disposición penal, o juego de disposiciones de la misma clase, castigando las especialidades de un particular uso indebido, o abuso informático. Así, ha introducido los llamados delitos informáticos, mediante la tipificación, artículo por artículo, de determinadas acciones que han sido objeto de sanción penal: la supresión, modificación y alteración de los datos contenidos en un sistema informático, trabar o falsear el funcionamiento del sistema; suprimir o modificar el modo de tratamiento o de la transmisión de los datos, falsificación de documentos informáticos. Sin embargo, las defraudaciones patrimoniales por medios informáticos quedan sin una específica regulación, siendo cubiertas por el artículo 441-1, que amplió el concepto de documento incluyendo el electrónico.

Según los autores consultados, probablemente ha sido Alemania, el país donde se ha ponderado con especial cuidado la conveniencia político-criminal de penalizar determinadas

conductas relativas a la informática, queriendo colmar una laguna legal inaplazable, según había denunciado la doctrina alemana. Las modificaciones efectuadas por la Segunda Ley para la Lucha contra la Criminalidad Económica, de 1986, en el Código Penal previendo las conductas delictuales relacionadas con los medios informáticos, no sólo consistieron en la modificación de algún precepto ya existente (párrafos 271, 273 y 348, en los que se agregaron las palabras datos, registros o almacenamiento), sino que se introdujeron una serie de nuevos tipos penales relativos a la delincuencia informática: el espionaje de datos, estafa mediante ordenador o fraude informático, falsificación de datos probatorios.

En Italia, el legislador estableció las disposiciones sobre delito informático en el Código Penal, usando la técnica legislativa de la extensión, esto es, elaboró una figura especial, paralela e inspirada en otras existentes, pero con relación a bienes nuevos como los sistemas informáticos, los datos y el software, y con nueva formulación de actos o acciones que proceden o son propios del ámbito informático. Se cubre el nuevo *modus operandi* a través de actos delictivos tradicionales.

V. SELECCIÓN BIBLIOGRÁFICA

1. ARÁNGUEZ SÁNCHEZ, Carlos; ALARCÓN NAVÍO, Esperanza. ***El Código Penal Francés traducido y anotado***. Granada, España, Editorial Comares, 2000, 370 p.
   Ubicación: Sede Valparaíso - MON, Monografía – 343.2(44) A662c.E 2000

2. CASTRO OSPINA, Sandra Jeannette (Profesora Titular de Derecho Penal - Universidad Externado de Colombia). ***Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano*** *[en línea].* Madrid, España, DelitosInformaticos.com, 15 de Julio 2002, p.
   http://www.delitosinformaticos.com/delitos/colombia.shtml

3. CHIARAVALLOTI, Alicia; LEVENE, Ricardo. ***Introducción a los delitos informáticos, tipos y legislación (Publicado en el Vl Congreso Latinoamericano en 1998, en Colonia, Uruguay. Publicado en La Ley, Nros. 202 del 23 de Octubre de 1998 y 215 del 11 de Noviembre de 1998, Argentina.)*** *[en línea].* Madrid, España, DelitosInformaticos.com, 02 de Diciembre de 2002, 32 p.
   http://delitosinformaticos.com/delitos/delitosinformaticos.shtml

4. CHILE. GOBIERNO DE CHILE. MINISTERIO DE JUSTICIA. ***Ciber delito en Chile: Normativa penal. Reunión de expertos en ciber delito OEA- Washington, 23-24 junio 2003*** *[en línea].* Washington, D.C., USA, Organización de los Estados Americanos, 2003, 15 p.
   http://www.oas.org/juridico/spanish/cybGE_IIIChi_Rep3.ppt

5. ***CÓDIGO PENAL Alemán StGB. Código Procesal Penal Alemán StPO***. Madrid, España, Marcial Pons Ediciones Jurídicas y Sociales, 2000, 429 p.
   Ubicación: Sede Valparaíso - MON, Monografía – 343.1/.2(430) C669p 2000

6. ***DELITOS INFORMÁTICOS*** *[en línea].* Madrid, España, Despacho de abogados Portaley.com,
   http://www.portaley.com/delitos-informaticos/

7. ***DELITOSINFORMATICOS.COM[11]: Mapa del Web*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, 1 p.
   http://delitosinformaticos.com/mapa.shtml

[11] DelitosInformaticos.com es un sitio español editado por un despacho de abogados, Portaley.com, para dar conocimiento de la legislación y los problemas legales existentes con las Nuevas Tecnologías.

8. ESPAÑA. ***LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*** *[en línea].* Madrid, España, Despacho de abogados Portaley.com, 2004, 30 p.
http://www.portaley.com/lssi/textoLSSI.shtml

9. ESPAÑA. ***LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2004, 16 p.
http://www.delitosinformaticos.com/descarga/lssi.pdf

10. FERNÁNDEZ DELPECH, Horacio. ***Protección jurídica del software: con comentarios de la legislación iberoamericana***. Buenos Aires, Argentina, Abeledo-Perrot, 2000, 244 p.
Ubicación: Sede Valparaíso - MON, Monografía – 34:681.3 F363p 2000

11. GARCÍA NOGUERA, Noelia. ***La legislación española frente a los delitos informáticos*** *[en línea].* Madrid, España, DelitosInformaticos.com, 15 de Julio 2002, p.
http://www.delitosinformaticos.com/delitos/legislacion.shtml

12. GARCÍA NOGUERA, Noelia. ***Delitos Informáticos en el Código Penal Español*** *[en línea].* Madrid, España, DelitosInformaticos.com, 15 de Julio de 2002, p.
http://www.delitosinformaticos.com/delitos/codigopenal.shtml

13. GONZÁLEZ RUS, Juan José (Catedrático de Derecho Penal - Universidad de Córdoba). ***Protección penal de sistemas, elementos, datos, documentos y programas informáticos (Revista Electrónica de Ciencia Penal y Criminología RECPC, 01-14-1999)*** *[en línea].* Granada, España, CRIMINET, Web de Derecho Penal y Criminología, 2004, 36 p.
http://criminet.ugr.es/recpc/recpc_01-14.html

14. HUERTA MIRANDA, Marcelo; LIBANO MANSSUR, Claudio. ***Delitos informáticos***. Santiago, Chile, Editorial Jurídica ConoSur Ltda., 1996, 377 p.
Ubicación: Sede Valparaíso - MON, Monografía – 343.3/.7(83) H887d 1996

15. JIJENA LEIVA, Renato Javier. Debate parlamentario en el ámbito del derecho informático: Análisis de la Ley Nº 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información. ***Revista de Derecho de la Universidad Católica de Valparaíso***, Valparaíso, Chile, XV, 1993/1994, pp. 347-401.
Ubicación: Sede Valparaíso – PP, Publicaciones periódicas –

16. JIJENA LEIVA, Renato Javier. Mociones parlamentarias en el ámbito del derecho informático. ***Revista de Derecho y Humanidades / Escuela de Derecho, Universidad de Chile***, Santiago, Chile, Vol. 1, Nº 2, 1992, pp. 218-250.
Ubicación: Sede Valparaíso – PP, Publicaciones periódicas –

17. ***LEGISLACIÓN SOBRE Delitos Informáticos: Argentina. Anteproyecto de Ley de Delitos Informáticos sometido a Consulta Pública por la Secretaria de Comunicaciones por Resolución No. 476/2001 del 21.11.2001*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, p.
http://delitosinformaticos.com/legislacion/argentina.shtml

18. ***LEGISLACIÓN SOBRE Delitos Informáticos: Chile. LEY relativa a Delitos Informáticos. Ley No. 19.223*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, p.
http://delitosinformaticos.com/legislacion/chile.shtml

19. ***LEGISLACIÓN SOBRE Delitos Informáticos: Costa Rica. Ley No. 8.148*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, p.
http://delitosinformaticos.com/legislacion/costarica.shtml

20. ***LEGISLACIÓN SOBRE Delitos Informáticos: Perú. Proyecto de Ley de Delitos Informáticos*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, p.
http://delitosinformaticos.com/legislacion/peru.shtml

21. ***LEGISLACIÓN SOBRE Delitos Informáticos: Venezuela. Ley Especial Contra los Delitos Informáticos*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2002-2004, p.
http://delitosinformaticos.com/legislacion/venezuela.shtml

22. MAGLIONA M., Claudio; LÓPEZ M., Macarena. ***Delincuencia y fraude informático. Derecho comparado y Ley Nº 19.223***. Santiago, Chile, Editorial Jurídica de Chile, 1999, 273 p.
Ubicación: Sede Valparaíso - MON, Monografía – 343.3/.7:681 M195d 1999

23. MENESES DÍAZ, Cristián Andrés (Abogado). ***Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno*** *[en línea].* Madrid, España, DelitosInformaticos.com, 30 de Septiembre 2002, 10 p.
http://www.delitosinformaticos.com/delitos/penalchileno.shtml

24. MANSON, Marcelo. ***Legislación sobre delitos informáticos*** *[en línea].*
http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

25. PALAZZI, Pablo Andrés. ***Delitos informáticos***. Buenos Aires, Argentina, Ad-Hoc, 2000, 272 p.
Ubicación: Sede Valparaíso - MON, Monografía – 34:681.3(82) P155d 2000

26. PIEDRABUENA RICHARD, Guillermo. Informe relativo a la diligencia e investigación de los delitos informáticos contemplados en la Ley 19.223 y al fraude informático contenido en el Oficio Nº 422 de 27 de septiembre de 2001. ***Boletín de jurisprudencia / Ministerio Público***, Santiago, Chile, Nº 6, Octubre 2001, pp. 86-105.
Ubicación: Sede Valparaíso – PP, Publicaciones periódicas –

27. PORTALEY NUEVAS TECNOLOGÍAS SL. ***La Legislación Española frente a los Delitos Informáticos*** *[en línea].* Madrid, España, DelitosInformaticos.com, 9 de Febrero 2004.
http://delitosinformaticos.com/legislacion/legisvsdelitos.shtml

28. ***PREGUNTAS FRECUENTES sobre la LSSI (FAQ´s)*** *[en línea].* Madrid, España, PORTALEY Nuevas Tecnologías, 2004.
http://www.portaley.com/lssi/preguntas.shtml

29. RAMÍREZ LÓPEZ, Ricardo Alberto.
http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml

30. REYNA ALFARO, Luis Miguel. El bien jurídico en el delito informático. ***Revista Jurídica del Perú***, Lima, Perú, Año LI, Nº 21, Abril 2001, pp. 181-190.
Ubicación: Sede Valparaíso – PP, Publicaciones periódicas –

31. REYNA ALFARO, Luis Miguel. Los delitos informáticos en el Código Penal Peruano. ***Revista Jurídica del Perú***, Lima, Perú, Año LII, Nº 31, Febrero 2002, pp. 61-73.
Ubicación: Sede Valparaíso – PP, Publicaciones periódicas –

32. ROVIRA DEL CANTO, Enrique. ***Delincuencia informática y fraudes informático***s. Granada, España, Editorial Comares, 2002, 693 p.
Ubicación: Sede Valparaíso - MON, Monografía – 343.3/.7:681.3 R875d 2002

33. SÁNCHEZ FRANCO, Alfredo. ***Delitos Informáticos y su Prueba. Algunas Consideraciones sobre la Ley Penal Mexicana, con base en la Legislación Penal Internacional*** *[en línea].* Madrid, España, DelitosInformaticos.com, 8 de Enero de 2004.
http://www.delitosinformaticos.com/delitos/ensayomexico.shtml

34. ***SERVICIO DE adecuación a la LSSI. Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico*** *[en línea].* Madrid, España, PORTALEY Nuevas Tecnologías, 2004.
http://www.portaley.com/lssi/

35. TÉLLEZ VALDÉS, Julio. ***Derecho informático***. 3ª ed., México, McGraw Hill/Interamericana Editores, 2004, 514 p.
Ubicación: Sede Valparaíso - MON, Monografía – 34:004.738.5 T275d 2003

36. UNIVERSIDAD DE EL SALVADOR. LANDAVERDE CONTRERAS, Melvin Leonardo; SOTO CAMPOS, Joaquín Galileo; TORRES LIPE, Jorge Marcelo. ***Delitos informáticos*** *[en línea].* Miami, Estados Unidos, e-libro.net, Octubre de 2000, 86 p.
http://www.e-libro.net/E-libro-viejo/gratis/delitoinf.pdf
http://www.monografias.com/trabajos6/delin/delin.shtml

37. VERA QUILODRÁN, Alejandro H. ***Delito e informática: (la informática como fuente de delito)***. Santiago, Chile: Eds. Jurídicas "La Ley", 1996, 279 p.
Ubicación: Sede - MON, Monografía –

38. VILLAHERMOSA IGLESIAS, Alfonso. ***Luces y sombras de la LSSICE: la regulación de Internet*** *[en línea].* Madrid, España, DelitosInformaticos.com, 2004.
http://www.delitosinformaticos.com/lssi/intro.shtml