MASTER DE PROPIEDAD INDUSTRIAL, INTELECTUAL Y NUEVAS TECNOLOGÍAS, EOI-FUNDACIÓN JOSÉ PONS. MADRID, 30 DE JUNIO DE 2008 .-

E s q u e m a

"Delitos Informáticos"

Eduardo de Urbano Castrillo
Doctor en Derecho
Magistrado del Gabinete Técnico
Tribunal Supremo

SUMARIO:

INTRODUCCIÓN.-

Antes de abordar el estudio de los delitos informáticos , nos parece importante destacar algunas ideas introductorias al tema:

* En primer lugar, hay que situar este fenómeno dentro de la sociedad de la información, que ha dado nombre a nuestra época y al mundo que nos ha tocado vivir.

La esencia de este mundo: instantaneidad, desaparición de las distancias y mayor productividad, influye sobre todos los órdenes de la vida, cambiando los modos de aproximarnos y de vivir en ella. Por eso se habla de una nueva cultura e incluso de una nueva revolución científica, propiciada por la electrónica y su aplicación informática.

No podemos detenernos más aquí, pero sólo diremos que entre los efectos de estas nuevas realidades, está el impacto que ha producido en el mundo del derecho: en los modos de trabajar, de acceder y gestionar la información y, como no, su repercusión en el mundo de la Justicia.

En este orden de cosas, por un lado, es cuestión de reconocer la trascendencia del fenómeno, capacitarse ante él y tener en cuenta que produce consecuencias negativas también: la delincuencia informática.

* En segundo lugar, queremos señalar en esta introducción la problemática legal existente en esta materia: carencia de un título específico en nuestro CP, sobre la "delincuencia informática" y la existencia de escasas fuentes internacionales.

Destacamos, en el segundo aspecto, la Convención del Consejo de Europa sobre el Cibercrimen, Budapest 23-11-2001, constituye el texto jurídico internacional más importante en materia de Delincuencia Informática.

Supone, sin duda, un instrumento jurídico del máximo interés para procurar una efectiva cooperación entre los Estados para combatir la delincuencia asociada a las nuevas tecnologías.

Sin embargo, y a pesar de sus aspectos positivos – aborda aspectos sustantivos y procesales, contiene definiciones y establece que "los Estados Parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias" (art.6.1)- su corto recorrido, pues entró en vigor el 1-7-2004, y el hecho de que aún no haya sido ratificada por países como Estados Unidos, China, Japón, Alemania o la misma España, hace que su impacto, por el momento, sea reducido.

* Otro dato que dificulta el conocimiento de esta materia es la constante innovación que se produce, pues los tradicionales medios de ataque, a base de "spam" (correos basura) y "gusanos", virus que colapsaban el sistema informático atacado, están siendo sustituidos por agresiones informáticas que buscan rendimientos económicos inmediatos: el "phising" (suplantación de la empresa que aparentemente está detrás del producto o bien ofertado) el "pharming" (clonación y redirección fraudulenta de páginas web de entidades financieras y comerciales electrónicas) o los "troyanos" (programas espías, que se apoderan de información sensible ajena).

Por otro lado, y según los expertos, las redes P2P (peer to peer) y países asiáticos como China y Corea, están cada vez más, detrás de estas nuevas modalidades de delincuencia informática, que hasta la fecha, procedía, en más de la mitad de los casos, de EEUU.

* Y por último, subrayar que nos encontramos ante un fenómeno de la máxima actualidad, como lo ponen de manifiesto recientes episodios de los que han dado cuenta los medios de comunicación en el último años.

Así, en Madrid, se ha detectado la existencia de una página web que enseña a destruir los parquímetros que está

instalando el Ayuntamiento en diversas zonas de la capital; o dos directivos de “La Ley”, exaltos cargos de “El Derecho” están siendo investigados por acceder , con la clave que tuvieron, a los sistemas informáticos de su antigua empresa, dificultando, al parecer, el acceso de los clientes de ésta, a dichas páginas, lo que se habría traducido en numerosas cancelaciones de contratos y los consiguientes perjuicios económicos para la editorial mencionada; o la condena de un Juzgado de Tarrasa a un *hacker* por utilizar en su favor la página web oficial del Festival de Eurovisión, desde la que solicitaba dinero a los visitantes.

Y más recientemente, un Juzgado de lo Penal condenó a dos informáticos por un delito de revelación de secretos al difundir a través de internet fotografías de explícito contenido sexual, en la que aparecían juntos una edil, el hermano del alcalde y una presentadora de televisión local, en lo que parecía tratarse de una “orgía” en toda regla , conducta que se realizó con la finalidad de que tales hechos fueran conocidos por los habitantes del municipio, habida cuenta de la relevancia pública de los afectados, en dicha localidad.

Además de ello, el Instituto Nacional de Tecnología de la Comunicación (Inteco), estima en más de 300.000 internautas el número de afectados por estafas en internet.

Y por último, gran parte de la controversia actual estriba en qué posible derecho tiene la empresa a controlar los correos eletrónicos y la navegación por internet de s sus empelados, lo cual produce un cruce de consecuencias jurídicas entre ambas partes, considerándose que si bien no hay delito por parte de la empresa, sí existe responsabilidad por parte de ésta si no existe base legal o reglas internas sobre control de uso de internet por parte de sus empleados, (STEDH 3-4-2007).

La problemática que examinamos, ofrece, por tanto, un interés indudable para adentrarnos en la tipificación de estas conductas y así, reflexionar sobre las cuestiones que plantea la realidad diaria.

Las abordaremos tanto desde el punto de vista procesal como sustantivo y comenzaremos por unas ideas generales sobre el delito informático, para examinar, seguidamente, los distintos delitos contenidos en nuestro CP.

I

I. EL DELITO INFORMÁTICO: ASPECTOS GENERALES

Antes de iniciar el examen de los distintos delitos informáticos, de un modo individualizado, es procedente referirse, aun con brevedad, a una serie de cuestiones generales sobre los mismos.

- ***Inexistencia de un título o rúbrica específica***

- ***Necesidad de establecer una regulación específica de la delincuencia informática***

-.***Problemas procesales***

Entre ellos:

-Dificultades de persecución

-Problemas de colaboración procesal

-Cuestiones de extraterritorialidad

-Cuestiones probatorias especiales

- Conceptuación general de estos delitos

- Naturaleza: delitos de riesgo (no requieren un resultado concreto), aunque los delitos tipificados en los art.256 y 264 pueden ser considerados delitos de resultado.
- Bien jurídico pluriofensivo :la intimidad informática, el derecho a la información, la defensa del patrimonio, la seguridad del sistema y otros más secundarios: derecho a la tranquilidad, a poder contratar, al ocio...
- Especial vinculación al aspecto económico : se ha dicho que se hallan vinculados a la informática, en cuanto a su medio comisivo y al mundo de los negocios, en cuanto a su desenvolvimiento.

- ***Clases de delitos informáticos***

a) Por la técnica de tipificación

b) Por los bienes jurídicos protegidos

II. LOS DISTINTOS DELITOS INFORMATICOS

Examinamos, seguidamente dichos delitos, de forma individualizada:

1) Art.197.2 (espionaje informático)
2) Art.238.5 (robo con fuerza tecnológica)
3) Art.248.2 (estafa informática)
4) Art.256 (ubicación abusiva de equipos terminales de telecomunicación)
5) Art.264.2 (daños)
6) Art.270 (propiedad intelectual)
7) Art.273-275 (propiedad industrial)
8) Art. 278.1 (secretos de empresa)
9) Art.560.1 (ataques a líneas o instalaciones de telecomunicación o correspondencia postal)

1)Artículo 197.

1. ***El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, 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 ficheros o soportes informáticos, electrónicos o telemáticos, o 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 o 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 un 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.

Es el "hacking". El ilícito informático más frecuente, y constituye el delito básico de riesgo informático. Se le conoce como "espionaje informático". ("Hacker" significa fisgón.)

La conducta punible es la interceptación de una comunicación electrónica, sin que sea necesario la revelación de su contenido.

El 197.2 tutela la libertad informática, cuya protección legal se contempla en el art.18.4 CE.

La conducta punible consiste en el apoderamiento, utilización o manejo de datos automatizados. Con dos requisitos: sin autorización del titular y en perjuicio de éste.

También incluye el acceder a esos datos o alterarlos, con el proposito de descubrir intimidades ajenas.

Como se puede preciar, no se castiga el mero intrusismo.

Objeto material: programas, datos de investigación, defensa, contabilidad, direcciones de clientes

Dinámica de la acción. En los años 80 se producía capturando passwords, y actuando a continuación. Hoy en día, infiltrándose en la red , conectándose a una línea telefónica ("pinchándola")

La jurisprudencia ha considerado que constituye el delito, la interceptación de un fax en el que una compañía hacía una oferta para construir un TAV para Corea del Sur, permitiendo así, a su competidora, presentar una oferta más ventajosa.

2)Artículo 238

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

5.Inutilización de sistemas específicos de alarma o guarda

Esta circunstancia representa la modernización efectuada por el CP 95 del clásico delito de robo con fuerza en las cosas.

Por “sistema de alarma” debemos entender aquél que mediante el sonido o la luz está concebido para denunciar un ataque al objeto o espacio protegido.

Y “sistema de guarda”, es aquél que permite custodiar el acceso a la cosa protegida.

La desactivación o inutilización del mecanismo de seguridad protector, con el objeto de asegurarse la huida, por ejemplo, no sería robo sino un hurto. Es evidente, no obstante, el problema de prueba que plantea el caso.

En cuanto al objeto material, se trata de una clase de robo, por tanto, de un ataque al patrimonio ajeno, cometido mediante el ejercicio de violencia sobre “sistemas específicos” de protección, no, en consecuencia, sobre los sistemas ordinarios, como el timbre, la aldaba o la campanita que suelen tener las puertas, para llamar.

De acuerdo con MUÑOZ CONDE, en este subtipo se integran tanto la alarma de un vehículo a motor, la que custodia un cuadro en un museo o las joyas en una joyería.

Se trata, pues, de sistemas electrónicos que actúan a modo de “llaves tecnológicas” propias de nuestra época, para facilitar el acceso a un lugar determinado, pues suponen una determinada combinación o clave prefijada, que se activa si se pretende acceder al lugar u objeto, sin anularla con la contraclave, correspondiente.

3)Artículo 248.

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

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

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. (Apartado añadido de acuerdo con la modificación establecida por la Ley Orgánica 15/2003, de 25 de noviembre)

Contempla el presente artículo, la “estafa informática”, la cual se inscribe dentro del concepto más general de los “fraudes informáticos”.

La “estafa informática” no encaja, en su dinámica comisiva, con la estafa tradicional pues no existe realmente engaño o error, dado que la máquina no goza de una sicología que pueda ser objeto de engaño.

Pero la nueva estafa, pivota sobre unos elementos distintos que guardan relación con la estructura clásica de la estafa: la manipulación informática o el empleo de “artificio semejante”, que equivale al engaño clásico; la transferencia no consentida , o acto de disposición de la estafa tradicional, y por supuesto, en ambos casos existe un perjuicio económico, que sufre el titular de la cuenta sobre la que se produce el ataque informático patrimonial.

No constituyen estafa informática, sino una estafa en la que se utiliza internet, los casos de :subastas en la red que no entregan el producto anunciado y pagado; prestación de “servicios fantasma” (viajes turísticos); productos “milagro” a precios costosísimos que no producen los efectos curativos que indican.

Por el contrario, entran en el art.248.2 aquellas estafas en las que el engaño se produce al sistema informático: apoderamiento de contraseñas de cuentas y acceso a productos que se pagan a costa del cuentacorrentista; o uso de tarjetas de terceros, con la que se adquieren toda clase de mercancias y servicios, etc.

El tipo requiere la realización de manipulaciones y el empleo de artificios dirigidos contra máquinas, para perjudicar a terceros.

Ahora es posible hablar de estafa, ya que existe una cobertura legal expresa, a pesar de la escasa precisión de los conceptos utilizados: “manipulación informática” y “artificio semejante”, pues el nuevo delito de estafa se construye con

dos elementos: manipulación informática y consecución, como resultado, de una transferencia de activos inconsentida.

La Jurisprudencia, recoge condenas por obtener una transferencia no consentida de activos en perjuicios de terceros, al manipular informáticamente o mediante un artificio semejante (aparentar ser el titular legítimo de la tarjeta), una tarjeta de crédito.

4)Artículo 256 ***. (Artículo redactado de acuerdo con la modificación establecida por la Ley Orgánica 15/2003, de 25 de noviembre)***

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses.

"Hurto de tiempo".

Acorde a su naturaleza de delito de resultado, requiere la producción de un perjuicio mensurable, y concreto, ya que debe superar los 400 euros, pues en otro caso, la acción será constitutiva de la falta prevista en el art.623.4 CP.

En la expresión "cualquier equipo terminal de comunicación" pueden incluirse el teléfono, el fax, el correo electrónico o el telex.

El tipo requiere, como elemento fundamental: la falta del consentimiento del titular del ordenador.

Se considera un desacierto, una norma desmesurada pues bastaría una sanción disciplinaria –si se produce en el ámbito de la función pública –o el despido –en el ámbito laboral de una empresa privada-. (En el ámbito militar, está considerado falta grave.)

La Jurisprudencia recogió el desvío de una línea telefónica destinada a pruebas , de uso exclusivo de los empleados de telefónica, hasta el domicilio del acusado desde el que se produjeron llamadas por importe superior a 1 millón de pesetas.

Una reciente sentencia de un juez de Nueva York, el juez John Spooner, ha dejado sin efecto el despido de un funcionario del Ayuntamiento de dicha ciudad , sustituyéndolo por una mera reprimenda, sobre la base de que es lícito

navegar por interne durante las horas de trabajo porque su uso hoy es similar a llamar por teléfono o leer la prensa.

La única condición es que se trate de un uso razonable, es decir, que no llegue a interferir en el resultado global de su rendimiento.

Quedan extramuros del presente tipo, los daños sobre el hardware, sancionable a través del delito de daños o sobre el software, para el que está previsto el art.264.2.. Y lo mismo, el simple acceso al sistema o el intrusimo de los "hackers" respecto a los cuales no se contabilicen daños o perjuicios económicos concretos.

5)Artículo 264.2

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el Artículo anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2.º Que se cause por cualquier medio infección o contagio de ganado.

3.º Que se empleen sustancias venenosas o corrosivas.

4.º Que afecten a bienes de dominio o uso público o comunal.

5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

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

Es el "cracking". Delito de "sabotaje informático", llamado también vandalismo informático, y que el CP español construye como un delito de "daños informáticos".

Bien jurídico protegido: la integridad de cosa ajena, materialmente valiosa, consistente en "datos, programas o documentos electrónicos", es decir lo que se conoce en la jerga informática como el *software* o elementos lógicos de los sistemas informáticos.

Los daños informáticos sobre los elementos materiales, básicos o periféricos (ordenador, pantalla, impresora...) entrarían en el delito básico de daños, porque el legislador no singulariza la protección del *hardware*, a diferencia de la que realiza sobre el *software*, en este art.264.2 CP.

Sujeto activo del delito puede ser cualquier persona distinta del titular de los datos, programas o documentos afectados por el sabotaje, que será el sujeto pasivo.

Por ello, si quien introduce el daño es el titular del programa, así para que se autodestruya en caso de impago, habrá de recurrirse a la legislación en materia de propiedad intelectual, no siendo aplicable el artículo 264.2.

El tipo es doloso pero el 267 no impide la condena por imprudencia grave siempre que los daños cuantificables excedan de los 80.000 euros.

Resultado: el daño, que puede ser la inutilización de un programa, requiere que ello sea consecuencia de que se dañe el hardware, lo cual puede suponer una imposibilidad o ralentización de operaciones, que por ejemplo se han de realizar a mano.

Como delito de lesión que es, el daño informático ha de ser real, no bastando la mera puesta en peligro (así virus que no logran su objetivo) por lo que su consumación exige una efectiva acción destructiva o alteradora de los datos o programas informáticos.

Su dinámica comisiva, incluye:

- el empleo de virus (programa contaminado que se actúa en cuanto se carga o incorpora en un ordenador, al “arrancar” el programa; suele venir con el correo electrónico)
- las bombas lógicas (uso de programas destructores)
- los “bugs” , destrucción de software aprovechando que los ordenadores utilizan otro programa, mediante un programa incompatible
- los “ping de la muerte”: envío de datos específicos a Windows 95 para que este programa se pare.
- Sabotaje de líneas telefónicas, incluso mediante su corte físico (así se paralizó el aeropuerto de Frankfurt en 1995)

6)Artículo 270**. **(Artículo modificado por la Ley Orgánica 15/2003, de 25 de noviembre)

1. ***Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 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.

2. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien intencionadamente exporte o almacene ejemplares de las obras, producciones o ejecuciones a que se refiere el apartado anterior sin la referida autorización.

Igualmente incurrirán en la misma pena 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 aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.

3. Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga 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 o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.

Ataques a la propiedad intelectual, en su dimensión patrimonial.

La tutela penal se realiza en un triple frente: los derechos de creación, los de explotación de la obra y la tipificación de actos de preparación como la fabricación, importación, circulación o tenencia de dispositivos para cometer dichos delitos.

Para poder captar la significación antijurídica formal del tipo,

Supone extender el objeto material protegido a las obras producidas o distribuidas a través de internet (musicales, bibliográficas, cinematográficas...).

Piénsese en la problemática que produjo el servidor musical *Napster* que facilitaba intercambios gratuitos de música bajada desde la red. Las querellas que le dirigieron Sony, Warner, Emi etc, pusieron fin al experimento y ahora lo normal es pagar , al titular del derecho, una pequeña cantidad para poder grabar un tema.

Conducta típica: la copia de programas y datos informáticos.

El número 3 del artículo castiga, igualmente, la mera fabricación, tenencia o introducción en el mercado de los mecanismos que permitan la reducción o eliminación de su protección.

Supone penalizar la superación ilícita de las barreras de protección de los secretos industriales (sistemas de seguridad de programas, códigos, encriptaciones...) para realizar las conductas que se tipifican.

7)Artículos 273-274 y 275

273

1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos

2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.

3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor.

Artículo 274.

1. Será castigado con la pena de seis meses a dos años de prisión y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, reproduzca, imite, modifique o de cualquier otro modo utilice un signo distintivo idéntico o confundible con aquél, para distinguir los mismos o similares productos, servicios, actividades o establecimientos para los que el derecho de propiedad industrial se encuentre registrado. Igualmente, incurrirán en la misma pena los que importen intencionadamente estos productos sin dicho consentimiento, 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 aquéllos se hayan adquirido directamente del titular de los derechos de dicho Estado, o con su consentimiento

2. Las mismas penas se impondrán al que, a sabiendas posea para su comercialización, o ponga en el comercio, productos o servicios con signos distintivos que, de acuerdo con el apartado 1 de este artículo, suponen una infracción de los derechos exclusivos del titular de los mismos, aun cuando se trate de productos importados del extranjero.

3. Será castigado con la misma pena quien, con fines agrarios o comerciales, sin consentimiento del titular de un título de obtención vegetal y con conocimiento de su registro, produzca o reproduzca, acondicione con vistas a la producción o reproducción, ofrezca en venta, venda o comercialice de otra forma, exporte o importe, o posea para cualquiera de los fines mencionados, material vegetal de reproducción o multiplicación de una variedad vegetal protegida conforme a la legislación sobre protección de obtenciones vegetales.

4. Será castigado con la misma pena quien realice cualesquiera de los actos descritos en el apartado anterior utilizando, bajo la denominación de una variedad vegetal protegida, material vegetal de reproducción o multiplicación que no pertenezca a tal variedad.

Artículo 275.

Las mismas penas previstas en el artículo anterior se impondrán a quien intencionadamente y sin estar autorizado para ello, utilice en el tráfico económico una denominación de origen o una indicación geográfica representativa de una calidad determinada legalmente protegidas para distinguir los productos amparados por ellas, con conocimiento de esta protección.

La tutela de la propiedad industrial tiene como objeto la protección de las creaciones industriales, es decir, los derechos inmateriales conectados a la actividad productiva, en cuanto poseen una importancia económica evidente.

Es sabido que en su ámbito, se incluyen las marcas, las patentes, los modelos de utilidad, los dibujos industriales, las topografías de los productos semiconductores, los títulos de obtenciones vegetales, las denominaciones de origen y las indicaciones geográficas representativas de una calidad determinada legalmente protegida.

En definitiva, los productos de la inventiva humana para su aplicación industrial o económica, siempre que se registren previamente y supongan una novedad sobre el estado de la ciencia en el momento de la creación.

Las conductas punibles, recogidas en los arts. 273 a 275 CP, tienen en común que se realizan sin consentimiento de los titulares de los derechos y que se encuentran previamente protegidos, por el Registro de la Propiedad Industrial.

A tal efecto, es preciso manejar, en todo momento, las leyes mercantiles básicas en la materia: Ley 17/2001, de Marcas; Ley 11/1986, de Patentes; Ley 11/1988, de Protección Jurídica de las Topografías de los Productos Semiconductores; Ley 3/1991, de Competencia Desleal; Ley 34/1988, General de Publicidad ; Ley 3/2000, de Protección de las Obtenciones Vegetales y Ley 20/2003, de Protección Jurídica del Diseño Industrial.

Serían impunes, las meras infracciones de obligaciones de orden civil en las que el infractor no persigue un beneficio económico , saltando, conscientemente, sobre las barreras protectoras ajenas que conoce –al menos, eventualmente-.

Resultan ajenas a la tutela penal, las conductas individuales, como la fabricación ilegítima de un utensilio para uso propio del "fabricante" o cuando existe una utilización de un producto patentado para fines sociales no económicos ("lucir bolso de marca", de imitación).

Es preciso, pues, una conciencia de aprovecharse, de enriquecerse con la acción aunque no se consiga despues, pues de lo que se trata es de desposeer a su legítimo titular, de los derechos exclusivos de propiedad industrial que pueda tener, con el fin de disponer o utilizarlos en cualquiera de las diversas formas que indican los preceptos penales (copiar, modificar, ofrecer a tercero, fabricar, comercializar, importar...).

Entrando ya en la *casuística*, sin duda, una de las cuestiones más interesante en el momento actual, es el de los conflictos entre "nombres de dominio" y "marcas".

Los *nombres de dominio,* ya sean de primer nivel genéricos (com.net.orgmil.int) o por países (es.uk.fr.) o de segundo, (edu.es, gob.es, etc), identifican a un titular que actúa en la red, dándose a conocer, ofreciendo información, sus productos, publicitándose o realizando transacciones económicas.

Pero “los dominios usados como cibermarcas en el mercado virtual, pueden infringir el derecho de exclusiva que otorga la marca” SAP civil Barcelona 23-4-01, por la sencilla razón de que el derecho de marcas, no excluye de su ambito protector “ninguna modalidad de comercio ni en concreto, el cibermercado”.

¿Cuál es o, cuál debe ser, la respuesta jurídica (penal) a esas posibles situaciones?

Algunos supuestos:

a) Ambito civil, sin relevancia penal:

- Registro de dominio de una marca registrada a nombre de otro titular. Siempre que exista riesgo de confusión, así por operar en el mismo objeto social, habrá derecho a ejercitar un a acción civil, para solicitar la anulación del dominio, el cese de la actividad y las indemnizaciones correspondientes.

- Competencia desleal. El aprovechamiento del crédito comercial y prestigio ajeno, para los propios intereses, así utilizando en una página web las excelencias de un competidor, que se utilizan en provecho propio. Es un típico caso de exigencia de indemnización y cese de la actividad.

- Publicidad ilícita. Entran en este apartado las infracciones a la Ley General de Publicidad (así art. 4), pero podrían tener relevancia penal en el supuesto del art. 282 CP, si pudieren causar “perjuicio grave y manifiesto a los consumidores”.

- Registro de nombre idéntico o similar, para revenderlo. Despues de algunos titubeos, los Tribunales dan la razón a la marca notoria (Casos Mac Donalds, Coca Cola, Panavisión...) , habiéndose establecido una norma específica para el tratamiento de esta cuestión, en USA, “Anticibersquatting Protection Act”.

- Coincidencias fortuitas. Se defiende (GRAGERA GALLARDO) al que registró el dominio , en base al

principio “first come, first served”. La solución no parece descabellada pero ,sin duda, exige matices, según el caso.

B) Ambito penal:

- Aprovechamiento indebido de marca notoria. Puede entrar en el art.274 CP, la comercialización de productos o servicios ,utilizando en la red esa marca, sin que los mismos se correspondan con los genuinos (SAP Madrid, 20-6-2001, “Caso Chase Manhattan”)

- Explotación de dominios ajenos. Se trata de atentados a la propiedad industrial tecnológica, aprovechándose de dominios ajenos, es decir con fines económicos, a través de técnicas diversas como el “word stuffing” , utilizar una determinada palabra , marca de un tercero, en una página web y de forma imperceptible para el ojo humano, al incluirla en el color idéntico al del fondo de la página; o el “deep link”, llevar al usuario a la página no inicial, controlada por un tercero, mediante un “linking” asociado a un “site” distinto y concreto.

8) Artículos 278-280.

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 al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del Artículo 197, 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.

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.

“Piratería informática”. O espionaje económico.

La conducta punible consiste en:

El apoderamiento de datos u objetos del sujeto pasivo, empleando alguna de las modalidades previstas en el art.197.1

Dicha acción puede realizarse de muy diversos modos: visualización, copia, transferencia informática, etc.

El concepto de secreto empresarial es eminentemente funcional, ya que el precepto protege la competencia económica antes que la intimidad, por lo que lo que es secreto en un momento suele dejar de serlo, en un momento posterior.

Hay que manejar, pues, criterios de utilidad y entidad, para la empresa , y tener en cuenta que el consentimiento, así la venta de un procedimiento tecnológico, por ejemplo, supone la desaparición del sentido de protección de la norma.

Su ámbito: las conductas de interceptación ilícita, de las comunicaciones en los sistemas informáticos o redes telemáticas de las empresas, donde se alojan documentos tan sensibles como su contabilidad , la cartera de clientes, los balances, los proveedores, proyectos estratégicos, procedimientos tecnológicos de producción, etc.

El "meterse" en el sistema informático de una multinacional, como "reto", sin apoderarse de información, es impune.

Los artículos 279 y 280 incluyen dos conductas más, que amplían los supuestos del sujeto activo: un subtipo agravado, en razón de que el autor estuviere legal o contractualmente obligado a guardar reserva, y un subtipo atenuado, para el caso de que la misma conducta la realizara quien no ha participado en la obtención del secreto.

9)Artículo 560.1

Los que causaren daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal, serán castigados con la pena de prisión de uno a cinco años.

Delito de desordenes públicos, en cuanto se causen daños de forma dolosa sobre líneas o instalaciones de telecomunicación o correspondencia vía postal.

Dentro de las modalidades actuales de "correspondencia postal", se incluye, sin duda, las líneas informáticas que son vehículo de la moderna correspondencia electrónica.

Modalidades o resultados delictivos que incluye:

-la destrucción (o perecimiento de la cosa)
-causar graves daños
-paralización del servicio
-producir una grave alteración del servicio

Sin duda el principio de proporcionalidad- la pena puede alcanzar los cinco años de prisión- demanda que se trate de conductas graves, fuera de toda duda (así, el artículo incluye verbos nucleares como *destruir, causar graves daños, paralizar un servicio o alterarlo gravemente).*

La producción de perjuicios económicos, consecuencia de acciones de dicho nivel, es evidente, y por eso debe incluirse , en el grupo de conductas delictivas informáticas de naturaleza económica.

III. ANEXO JURISPRUDENCIAL

Entre las sentencias más recientes dictadas en relación a la delincuencia informática , tenemos las siguientes:

- *STS nº 237/2007 de 21-3-2007*
- *STS nº 109/2006 de 8-2-2006*
- *STS nº 1557/2004 de 30-12-2004*
- *STS nº 1476/2004 de 21-12-2004*
- *STS nº 807/2003 de 3-6-2003*
- *STS nº 948/2002 de 8-7-2002*
- *STS nº 1461/2001 de 11-7-2001*
- STS nº 1861/2000 de 4-12-2000.
- STS nº 1532/2000 de 9-10-2000
- STS nº 1599/1999 de 15-11-1999
- STS nº 234/1999 de 18-2-1999
- STS nº 584/98 de 14-5-1998

Y además, STS 369/2007, de 30-4 y STS9-5-2007. La primera , que considera atípico el acceso al correo electrónico de un funcionario de baja, y la segunda que considera delito de falsificación de moneda falsa –no, un delito informático- la introducción de un PIN sustraído a su titular para clonar tarjetas.

(STS nº 237/2007 de 21-3-2007)

Esta reciente sentencia se ocupa de un delito de revelación de secretos del art.197.1 CP cometido por un marido que a la vista de que las facturas mensuales por utilización de internet se disparaban hasta 70 horas de consumo al mes, adquirió un programa eBlaster para poder comprobar desde su ordenador particular instalado en su domicilio , quién lo utilizaba. Para ello, lo instaló de tal modo que cada 30 minutos se volcara copia de todas las comunicaciones telemáticas que se realizaban sobre su cuenta de correo electrónico. Y así pudo saber que la usuaria era su esposa que entraba en chats de casados/infieles con conversaciones de tipo sexual y averiguó que tenía una pareja.

El condenado afirmó que sólo pretedía obtener pruebas para el procedimiento matrimonial que se disponía a entablar pero la conducta despegada suponía un ilícito apoderamiento de comunicaciones privadas , a través de internet, lo cual se integra en el delito por el que fue condenado.

Resulta de interés, igualmente, señalar que se le apreció una atenuante analógica del art.21.6 en relación con el art.21.3 al apreciar una menor culpabilidad ya que alegó que si bien no podía desconocer la ilicitud de su proceder, su finalidad no era tanto atentar a la intimidad de su esposa como proteger a la hija de ambos.

(STS nº 109/2006 de 8-2-2006)

Trata esta sentencia del delito de daños informáticos previsto en el art.264.2 CP.

Los hechos probados refieren la conducta de un administrador de hecho de una empresa, que al comunicársele que debía abandonar la sociedad, “con el fin de perjudicar a la empresa”, realizó diversos hechos, entre los cuales se incluye que “dañó archivos y discos duros de los ordenadores, ocasionando desperfectos en los mismos por valor de 2.203.000 pesetas”.

El acusado, condenado por el delito arriba indicado, combate la condena en casación, negando la existencia de prueba de su autoría.

El Tribunal Supremo considera “un hecho evidente” la realidad de dichos daños en el sistema informático de la empresa de la que fue despedido, pues “*la Sala (enjuiciadora) tuvo a su disposición elemento, evidentemente incriminatorio, derivado de las dificultades para restaurar el sistema y las complicadas operaciones que tuvieron que realizar para recuperar la información*”, y que tales daños fueron obra del recurrente, al igual que los otros delitos de coacciones y societario, a que también fue condenado, en atención a la variada prueba de que se dispuso.

Más allá de la cuestión de prueba apuntada, no hay en la sentencia , estudio alguno del tipo delictivo, que a la vista de los hechos y de que no se combatió su calificación , no merecieron mayor atención, en vía de recurso de casación.

(STS nº 1557/2004 de 30-12-2004)

La presente sentencia resulta de interés , por los hechos en sí, que muestran una de las modalidades de estafa relacionada con el mundo de las nuevas tecnologías, en concreto, cuando la propia instalación de un sistema informático diseñado para la operativa empresarial, está en el origen de este tipo de conductas delictivas.

Los hechos son como siguen: “*A): 1) El acusado Emilio Rafael M M, nacido el 21-3-55, sin antecedentes penales, en representación de la entidad Proyectos Virtuales Multimedia, S.L., hizo anuncios en medios de comunicación con los logotipos “Páginas virtuales” “ITS Telecom., S.L.”, y Telefónica –Grupo distribuidor-, en los que ofrecía una selección de personas por todas las provincias, a fin de ofrecer en su zona servicios de alta tecnología especialmente diseñados para empresas, sobre la base de que los técnicos de aquélla entidad se encargaban de formar y proporcionar todas las ayudas necesarias para el desarrollo de la actividad, y que dichas personas obtendrían una rentabilidad inmediata, servicio en exclusiva y elevada remuneración, más 8 millones de pesetas al año si la dedicación era exclusiva.- 2) Algunas personas se interesaron por los anuncios y se pusieron en contacto con el acusado, manteniendo diversas reuniones y recibiendo aquéllas información e impresos aclaratorios respecto al producto que ofrecía la expresada entidad, entre ellos uno con logotipos Páginas Virtuales y Telefónica –Grupo distribuidor-, relativo a la contratación del cliente para su inclusión en*

"Páginas Virtuales", en cuya cláusula quinta se dice "P.V.M., S.L., cuidará del correcto y continua funcionamiento de la red que le es propia, no haciéndose responsable de los posibles cortes imprevisibles que no dependieran de su sistema, quedando obligado a restablecer el servicio en la mayor brevedad posible".- Asimismo Páginas Virtuales se comprometía a confeccionar dos páginas Web a cada cliente, reservándole espacio para otras 200 aproximadamente, todo ello de forma gratuita y cada página adicionada a las dos primeras con un coste de 5.000 ptas cada una –folio 27-; en algún anuncio Páginas Virtuales ofrecía desde Granada un completo servicio de acceso a Internet para empresas, y de se decía que lo único que tenía que pagar la empresa era su presencia en el CD-ROM que se confeccionaría –folio 90-, y el cliente, mediante el pago de una cuota anual tendría derecho, entre otros, a la confección de 2 pantallas Web y el uso de los servicio de Internet –folio 176-.- 3) Proyectos Virtuales Multimedia, S.L., no tenía contrato alguno con Telefónica que le autorizara a usar el logotipo de ésta, el producto que ofrecía era propio y sin que en el mismo tuviera Telefónica intervención alguna.- 4) Las personas que más adelante se dirán, confiadas en que en la documentación que se les entregó aparecía el logotipo Telefónica y también en los anuncios que el acusado hizo, así como que en las conversaciones habidas siempre se aludía a Telefónica, decidieron adquirir el producto, concertando los oportunos contratos, en los que figuraba Proyectos Virtuales Multimedia S.A. como propietaria de Páginas Virtuales que amparaba una serie de servicios ofrecidos a empresas mediante su inclusión en un programa por ordenador distribuidor en un CD ROM de edición anual, la cual cedía en exclusiva la comercialización de las zonas que, en cada contrato especificaban y por el precio que se decía; en el pacto Tercero se acordaba, entre otros extremos, "que el titular –el adquiriente- una vez abonado el precio pactado... se obliga a realizar todas las gestiones necesarias para conseguir el mayor número de adhesiones al servicio ofertado por P.V.M. a través de "Páginas Virtuales".- Para ello habrá de dotarse de: Local para oficina, Ordenar P.C. con programas de gestión y tratamiento de imágenes, escáner, impresora, material de papelería...", con una inversión mínima de 2.500.000 ptas, esto último, según uno de los anuncios –folio120-; en el pacto quinto se decía que "si transcurridos tres meses desde la firma del presente contrato, el titular –adquirente- no consiguiera una media de 150 contratos mensuales, P. V. M. tendrá plena autonomía para intervenir directamente en la suscripción de nuevos usuarios en el ámbito de aplicación del presente

contrato, sin que el titular tenga derecho por ello a percibir ningún tipo de pago o indemnización sobre el importe de la facturación obtenida en dicha intervención..., sin que por ello sufra el titular pérdida o menoscabo de los derechos adquiridos en este contrato"; en el pacto sexto se decía que "P.V.M. se compromete a realizar el trabajo y desarrollo de un CD ROM anual conteniendo la información referente a la zona en cuestión---" y también que pondría "a disposición del titulara – adquirente- cuantos medios sean necesarios para el buen desarrollo de la actividad, y en especial los medios técnicos de acceso para los usuarios enclavados en su zona de actividad".- Las indicadas personas son las siguientes: 1) Joaquín S I y José Manuel R R, en representación de T S.L., suscribieron un contrato de fecha 1-6-2000, adquiriendo en exclusiva 4 zonas de Sevilla por un precio total de 6.000.000 de pesetas – 1.500.000 por zona-.- 2) Gabriel F O, en representación de Aplicaciones Básicas de la Comunicación S.L., adquirió una zona de Jaén 2, precio 1.500.000 ptas, y en la zona Jaén 1, por igual precio, según contratos de fecha 1-5-2000 y 3-4-2000.- 3) Mª del C G L, adquirió zona de Cádiz, precio 1.500.000 pts. Según contrato de 13-6-2000.- 4) María de los Angeles G P adquirió zona de Valencia por precio de 1.500.000 pts, según contrato de 20-6-2000.- 5) Juan Diego B T, en virtud de contrato de 1-6-2000, adquirió zona de Córdoba 1, por precio de 1.500.000 pts, y otro contrato en igual fecha y precio por la zona de Córdoba 2.- 6) Javier A C, en virtud de contrato de 23-5-2000 adquirió zona Ciudad Real y Provincia por precio de 1.500.000.- 7) Carlos C B adquirió zona de Madrid por el precio de 4.650.000, según contrato de 14-2-2000 abonando solo 1.200.000 ptas.- 8) Empresa Virtual G, S.L. representada por Miguel Angel C G, adquirió zona de Valencia 5, precio 1.500.000, según contrato de 28-9-2000.- 9) Margarita L C adquirió zona de Albacete y provincia por precio de 1.500.000 ptas, según contrato de 10-5-2000.- B): El acusado, en representación del I.T.S. Telecom, S.L., tras anunciarse igualmente en medios de comunicación, con los anagramas de dicha empresa y Telefónica –Grupos distribuidor-, contrató la venta de igual producto, haciendo constar que pertenecía al grupo distribuidor de Telefónica y como tal comercializaba los servicios ofrecidos por la misma, así como que era propietaria de la marca Páginas Virtuales, vendió dicho producto a las siguientes personas: 1) A María del Carmen A D la zona de Granada capital provincia por el precio de 775.000 ptas, según contrato de 19-1-2000.- 2) Santiago M P la zona 1 de Málaga por el precio de 775.000, según contrato de 19-1-2000 y por contrato de igual fecha y precio la zona 2 de Málaga.- 3) A

Manuel Jesús J R la zona Cádiz 1 por el precio de 775.000 ptas, según contrato de 1-1-2000, y otro contrato de igual fecha y precio por la zona 2 de Cádiz.- La citada empresa ITS Telecom., S.L. tenía concertado un contrato con Telefónica de fecha 1-1-2000 que tenía por objeto la mediación de aquélla en el contratación entre el cliente y Telefónica de España. De lo equipos y servicio de telecomunicaciones por la que el agente estaba habilitado de acuerdo con el Anexo I del contrato, anexo que no consta en las actuaciones, pero sí que los equipos y servicios serán contratados pro Telefónica y el cliente final, con al mediación del agente –la citada empresa-, tratándose en definitiva de productos de Telefónica y no de dicha empresa.- C): Las personas que contrataban con las entidades que representaba el acusado, intentaron captar clientes, consiguiendo, a veces, algunos, pero al pretender hacerles a ellos y a otras más una demostración práctica, sólo en aisladas ocasiones consiguieron acceder a alguno página Web y en males condiciones, algún otro lo consiguió al principio, pero en al generalidad de las veces no obtuvieron resultado alguno, lo que les impidió hacer contrataciones y dejar sin efecto algunas de las llevadas a cabo.- D): El acusado carecía de medios para facilitar los recursos técnicos a que se obligó, lo que conocía cuando contrató.- E/: Todos los adquirentes pagaron el precio convenido, salvo Carlos C B que sólo abonó 1.200.000 ptas.-"

El importe de las cantidades entregadas por los clientes superó los 50 millones de pesetas.

La otra cuestión de interés de la sentencia es el abordaje de las cuestiones jurídicas, y más en concreto, de si hubo una estafa. El Tribunal Supremo estima el recurso y revoca la condena de instancia, sobre la base de que "*no se trataba...de un falso "invento" o "fachada" creada fuera de toda realidad con el único fin de engañar a otras personas....(pues) si el producto existía y alguna, aunque evidentemente insuficiente infraestructura tecnológica, se dispuso a llevar adelante el negocio, es atrevido afirmar el ánimo de engañar*".

La Sala casacional considera que existió un "mero incumplimiento de obligaciones", ya que sólo se ha probado dicho incumplimiento contractual, reprobable jurídicamente pero no punible, pues:

"*no fue, en absoluto, ninguna invención el que el recurrente era creador de un producto, identificado como*

"páginas amarillas virtuales",ya que ese producto tuvo existencia comercial en la ciudad de Córdoba, por lo que en principio, no debe sorprender el que se intentase su extensión, mediante el régimen de franquicias, hacia otras zonas y que, eso sí, posteriormente Emilio Rafael no cumplió adecuadamente con las obligaciones que había contraído con aquellos que ya le habían entregado diversas sumas de dinero por causa de ese negocio. Por todo ello resulta que el acusado...simplemente, (ha) incumplido una promesa".

(STS nº 1476/2004 de 21-12-2004)

Examina esta sentencia el delito de estafa informática (art.248.2 CP), que es sin duda, el delito informático que hasta el momento ha llegado en más ocasiones al Tribunal Supremo.

Los hechos, sinteticamente, son los siguientes: el hijo de los propietarios de un establecimiento de deportes, irrumpe de madrugada en el mismo, acompañado de una joven, manipulando el TPV (Terminal Punto de Venta), fingiendo ventas que cargaban en la tarjeta Visa de la joven, a la cual, en forma de supuestas devoluciones, se le ingresaron unos 52 millones de pesetas.

La sentencia considera que estamos ante un delito de estafa informática del art.248.2 CP, ya que el autor se ha valido de "alguna manipulación informática", como requiere el subtipo.

También se examina quien sea el sujeto pasivo de este delito, concluyéndose que lo es el titular del patrimonio perjudicado, el Banco , aunque finalmente sean los padres de uno de los condenados, los que hubieron de responder civilmente.

(STS nº 807/2003 de 3-6-2003)

La presente sentencia también examina un caso de "estafa informática", en el cual se trata el interesante tema del engaño, ya que en el delito de estafa, al tratarse de un delito relacional, entre personas, es claro que el engaño lo debe producir el agente a la victima.

Sin embargo*, "cuando la conducta se realiza frente a una máquina, mediante las formas comisivas del art.248.2 CP nos encontramos con la denominada estafa informática".*

En el presente caso, si bien no es posible engañar a una máquina, hay una apariencia de titularidad de una persona hacia otra, a la que se engaña, usando una tarjeta electrónica que correspondía a otra persona.

(STS nº 948/2002 de 8-7-2002)

En la sentencia en cuestión, se trata de un delito de falsificación de moneda, cometido mediante el llamado "dinero de plástico", al copiar el contenido de las bandas magnéticas de tarjetas de crédito de sus titulares, y realizar nuevas tarjetas, a nombre del acusado. Para, a continuación, realizar diversos pagos, en diferentes establecimientos comerciales.

Se trata de un delito de falsificación/fabricación de moneda, del art.386 1º del CP, al haberse confeccionado tarjetas mendaces mediante la sustitución de los datos auténticos contenidos en la banda magnética de las mismas.

"Fabricar" equivale a confeccionar "ex novo", por lo que el verbo nuclear del delito encaja perfectamente en el artículo mencionado, según Acuerdo del Pleno de la Sala Segunda del Tribunal Supremo de 28-6-2002

.

Por otro lado, no estamos ante un delito del art.248.2 CP ya que una cosa es *"que se manipulen sistemas informáticos para defraudar, y otra, completamente distinta, que se confeccione una tarjeta mediante la incorporación falsaria de datos de origen o producción informática para, con ella, posteriormente, levar a cabo actos fraudulentos".*

(STS nº 1461/2001 de 11-7-2001)

Esta sentencia, aunque dictada en aplicación del art.197 CP, tiene, en base a los hechos, connotaciones económicas y por eso se incluye.

Se trata de un funcionario del Ayuntamiento de Madrid, que utilizando la clave informática de una auxiliar a sus órdenes, obtiene cerca de cuarenta hojas del padrón correspondiente a diversas personas , con sus datos personales, con destino final que no pudo establecerse.

Los hechos se incardinan en un delito de descubrimiento de secretos del art.197.2 CP, ya que el condenado obtuvo

información confidencial, amparada por la LORTAD de 29-10-1992, sin competencia para ello ni lo hizo en la forma reglamentariamente establecida.

La sentencia, analizando la cuestión, indica que con tal artículo "*se trata de poner freno a los abusos informáticos contra la intimidad, es decir, contra aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento queda reservado a su titular*"

El "perjuicio" que exige el tipo consiste, simplemente, en el daño que se causa al perjudicado, al poner al descubierto aspectos personales del sujeto afectado sin su consentimiento.

Por otro lado, al no distinguir la LORTAD, todos los datos personales automatizados quedan protegidos por la conminación punitiva del art.197.2 CP. Y los datos de los que se apoderó el condenado, tienen carácter reservado o secreto, es decir, no destinados a ser objeto de libre publicidad (nombres y apellidos, fecha y lugar de nacimiento, DNI, dirección, teléfono, familiares convivientes, estudios realizados y otros datos en clave).

(STS Nº 1861/2000, DE 4-12-2000)

Esta sentencia, se refiere a la conducta de diversos funcionarios –de la SS y del CNP- que facilitaron informaciones sobre personas físicas y jurídicas , cuya identidad conocían en función de su acceso a bases de datos informáticas, por razón de sus cargos, las cuales entregaban, a cambio de precio, a financieras, empresas, despachos de abogados, agencias de detectives, etc- .

En razón de ello, fueron condenados como autores de delitos de cohecho y revelación de secretos .

En cuanto a las afirmaciones más interesantes que se contienen en la sentencia, relacionadas con la conducta y delitos mencionados, pueden destacarse las siguientes:

" *se trataba de informes sobre las incidencias de la vida laboral de los afiliados a la Seguridad Social que se extraían del sistema informático de ese organismo, contenido que notoria e implícitamente, conlleva un carácter reservado de innecesaria reiteración dado que*

su propia naturaleza, origen y destino determina dicha consecuencia legal."

"en cuanto al disco duro del ordenador de P., su presencia y contenido avalan –en contra de lo que se afirma en el Recurso- la credibilidad del referido testimonio del coacusado ya que, segú se dice en la combatida resulta"significativo que cuando se practica un registro en las oficinas de P., todos los datos, documentos y archivos habían desaparecido, aunque pudo contrastarse a través del disco duro la conformidad de los datos obtenidos en el registro efectuado a C. Con los extraidos del disco duro de P".

"el recurrente conocía la cualidad de funcionario de la seguridad social de C., lo que implica el conocimiento de que la fuente de los datos que éste le proporcionaba no era otra que el sistema informático de la seguridad Social y que la posibilidad de acceso a tales datos radicaba en dicha cualificación".

"en la redacción que se da al art.367 por la LO 9/1991, no se habla ya de secreto, sino de informaciones, que no deban ser divulgadas. Deber de no divulgación que, en cuanto se refiere a determinados datos del Sistema de la Seguridad Social, está expresamente proclamado en el art.30 del texto refundido de su Ley General".

Por último, resulta de interés, aunque no se desarrolle la afirmación, el hecho de que se indique sobre "*los listados informáticos"* a que se refiere el recurrente en su alegación del apartado tercero, que *"dichos listados carecen de valor probatorio" .*

(STS Nº 1532/2000, DE 9-10-2.000)

La sentencia trata del delito de descubrimiento de secretos, del art.197 párrafo 5º y 6º CP, en un caso en que, tras irrumpirse en el despacho del Presidente de una Asociación de parapléjicos y grandes inválidos, para apoderarse de licencias de programas informáticas, así como CDS con programas originales –Windows 95 y Microsoft Office- se revelaron datos de los integrantes de

dicha Asociación, de carácter personal, que revelaban el estado de salud y minusvalía física de dichos miembros, sus domicilios, teléfonos, cuentas bancarias, etc, a fin de ofrecerles, como se dice en el *factum,* actividades de contactos, sexo o "trabajos fraudulentos" .(sic)..

Dado el carácter de los datos sobre los que recayó la actividad delictiva, se aplicó el inciso final del último párrafo del art.197 del CP, esto es, cuando la revelación de secretos se realiza con fines lucrativos y además, afecta a datos de carácter personal que revelen la ideología, religión creencias, salud, origen racial o vida sexual, o la victima fuese un menor o incapaz).

Igualmente, se recoge que "*el acusado actuó voluntariamente con plena conciencia del carácter reservado de los datos y de la invasión a la intimidad que representaba su apoderamiento no autorizado con ánimo de indebida utilización"*

(STS Nº 1599/99 DE 15-11-1.999)

Sentencia que condena a los autores, varios técnicos y funcionarios, como responsables de un delito de revelación de secretos y otro de cohecho por proporcionar a diversas personas físicas y jurídicas datos sobre la vida laboral de trabajadores incluidos en los ordenadores del INSS.

De nuevo la conexión entre un delito que protege la intimidad de las personas y otro de naturaleza económica, aparece evidente.

El interés de esta resolución estriba tanto en la magnitud de los hechos –pues afectaron a más de 20.000 consultas que a 2.500 ptas cada una, las sencillas, y 7.500 si ofrecían "multiservicio", suponían 10 millones quinientas mil pesetas- como en los problemas procesales suscitados, sobre la prueba de los mismos.

En efecto, en el recurso –desestimado íntegramente , a pesar de contener 13 motivos- se critica la omisión, en la sentencia de instancia, de pronunciamiento sobre el "volcaje de datos" procedentes del ordenador de la empresa en la que trabajaba uno de los condenados y que habría sido realizado

por la policía sin las garantías derivadas del art.24.1 CE y 5.1 LOPJ, al no haber estado presente el secretario y carecer de la menor garantía judicial, que impidiera su manipulación, al haberse depositado los ordenadores y disquetes, en el depósito de la Delegación Provincial de Informática.

La sentencia es de gran interés tanto por lo que dice como por lo que insinúa. Así, y empezando por esto último, afirma que "*todo el esfuerzo empleado para mantener la nulidad de las pruebas se debió llevar por otro cauce o por la vía de la nulidad casacional denunciando la infracción de las formalidades esenciales exigidas para su práctica y acreditando que le había producido indefensión. La vía del quebrantamiento de forma por incongruencia omisiva –la seguida por el recurrente- es más limitada y se reduce a comprobar si ha habido respuesta , acertada o desacertada, a las cuestiones jurídicas suscitadas por las partes."*

En efecto, sobre el tema del "volcaje de datos", la Sala se pronuncia en el siguiente sentido: "*su práctica se llevó a cabo con todas las garantías exigidas por la ley. En primer lugar, la entrada y registro se realizó de forma correcta y con la intervención del Secretario Judicial que cumplió estrictamente con las previsiones procesales y ocupó los tres ordenadores, los disquetes y el ordenador personal. Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos , identificando su origen y procedencia".*

Sin embargo, en la mentada resolución , se añaden dos observaciones, enteramente razonables aunque sin consecuencias materiales para el recurso, : por un lado, la parte recurrente, pudo solicitar una contrapericia, cosa que no hizo, a pesar de tener a su disposición durante toda la fase de instrucción, el material probatorio; y por otro, habría sido conveniente que el Juez de Instrucción, de igual manera que sucede en el artículo 348 de la LECRIM, ofreciera a la parte interesada la posibilidad de designar otro perito que presenciase la operación y pudiera solicitar una contrapericia.

(STS Nª 234/99 DE 18-2-99)

Se trata en esta sentencia de la actuación de un periodista que obtuvo, por procedimientos no esclarecidos, *"un listado del archivo informátizado donde estaban registrados los enfermos de (una) Prisión y otro en que figuraban los internos destinados en la cocina"*, y comprobando que al menos dos –con SIDA- coincidían en ambas listas, reveló con nombres y apellidos la identidad de los mismos, y elaboró un reportaje criticando la situación y censurando a las Instituciones Penitenciarias por tamaña negligencia.

Con independencia del resultado del proceso –la Audiencia le absolvió del delito de revelación de secretos que se le imputaba, al aplicar la eximente de ejercicio legítimo de un derecho-, en decisión que la Sala Segunda revocó, condenándolo como autor de dicho delito, al apreciar únicamente, de forma incompleta, la mencionada eximente, es interesante lo que se dice en torno al art.197.2 CP.

Dicho artículo –afirma la sentencia- describe el tipo básico de los recientemente llamados por la doctrina "delitos contra la libertad informática" o "habeas data", esto es, de los delitos que atentan contra la intimidad de las personas ,desvelando o, más ampliamente, haciendo un uso ilegítimo de los datos personales insertos en un programa informático".

Siendo el objeto de la acción delictiva "*datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado".*

Añadiéndose, una vez enunciados los distintos soportes en que se pueden contener esos datos, que *"el delito se consuma tan pronto el sujeto activo "accede" a los datos, esto es, tan pronto los conoce y tiene a su disposición, pues sólo con eso se ha quebrantado la reserva que los cubre"* pero que exige la producción de un perjuicio, el cual se produce siempre que trasciende de la privacidad de la persona y de su núcleo familiar, entendido esto dentro de los parámetros del hombre medio de nuestra cultura.

(STS Nº 584/98 DE 14-5-98)

La presente sentencia se refiere a un caso en que el acusado, en su condición de funcionario de la Tesorería de la Seguridad Social de Alicante y Jefe del Area de Recaudación, utilizando su clave de acceso personal y su contraseña particular del terminal informático del citado órgano, consultó datos de la cuenta de cotización de una sociedad mercantil sobre las transacciones de deuda de cuenta de cotización y las de la deuda histórica , imprimió dicha información y la facilitó a un grupo político del Ayuntamiento en que era Alcalde quien había sido administrador de la referida sociedad, lo cual sirvió para que el mencionado grupo presentara una acción penal con la base documental referida..

Dichos hechos integran el delito del art.367 párrafo primero del CP de 1973 , es decir, revelación de secretos, fundada en la divulgación de una documentación informática referida a datos de orden fiscal y económico que, por su naturaleza y por ser de obligada comunicación a la Administración Pública, están amparados por el secreto, respecto a terceros, como dijera la STS de 21-5-93.

Es también destacable, que la prueba del delito , ante la ausencia de otras de tipo directo, se basa en las exigencias de la prueba indiciaria, cumplidas en el caso, como se detalla: "*a) los datos revelados se obtuvieron de los archivos informáticos de la Oficina en la que trabajaba el acusado…b) En el rastreo realizado posteriormente por los servicios informáticos aparece una sola consulta de esa clase, es decir, sólo una vez se hizo una consulta que abarcara todos esos datos de la referida empresa, c) la consulta se realizó con la clave personal y el código de acceso que precisamente corresponden a los del*

acusado, d) la consulta se produjo a la una de la tarde del día nueve de noviembre y e) El acusado ha reconocido haber realizado en ese tiempo consultas sobre la referida mercantil".

Pues bien, continúa la sentencia. *"A partir de tales datos la conclusión de que fue el acusado quien hizo tal consulta y, una vez impresa, la pasó a terceros constituye una deducción asentada en datos objetivos declarados probados, plurales, concomitantes e interrelacionados, y que responden a las reglas de la lógica y de la experiencia".*

IV. REFERENCIA BIBLIOGRAFICA

Son ya muchas las obras existentes sobre la problemática de la "Delincuencia Informática". Además, y como es natural, todas ellas, remiten, a su vez, a otro numeroso catálogo de libros sobre la materia.

Hecha la advertencia, nos permitimos indicar las siguientes:

- "Delitos contra y a través de las nuevas tecnologías.¿Cómo reducir su impunidad?", dtor.*Eloy VELASCO NUÑEZ, CGPJ, 2006.*
- "El fraude y la estafa mediante sistemas informáticos", de *Alfonso GALÁN MUÑOZ, Tirant lo blanch, 2005*
- "Responsabilidad penal y civil por delitos cometidos a través de Internet", de *Manuel GOMEZ TOMILLO, Aranzadi, 2004.*
- "Prevención y detección de delitos informáticos" de *Debra LITTLEJOHN SHINDER, Anaya Multimedia, 2003.*
- "Internet y Derecho Penal", Director *Juan José LOPEZ ORTEGA. CGPJ, 2001.*
- "Delincuencia Informática y Derecho Penal" *de Ricardo M.MATA Y MARTÍN. Edisofer, Madrid, 2001.*
- *"*Criminalidad informática:una introducción al cibercrimen", *Ricardo M.MATA Y MARTÍN,* Actualidad Penal, 6-12 octubre 2003.
- "Internet y Delitos contra la propiedad intelectual", de *Fernando MIRÓ LLINARES , Iberautor Promociones Culturales.*

- "Delincuencia Informática. Problemas de responsabilidad", Director *Oscar MORALES GARCÍA, CGPJ, 2003.*
- "Internet y Derecho Penal*: Hacking y otras Conductas Ilícitas en la Red" de Esther MORON LERMA. Aranzadi Editorial, 1999*
- "Delitos informáticos y delitos comunes cometidos a través de la Informática"de *Enrique ORTS BERENGUER* y *Margarita ROIG TORRES, Tirant lo blanch, 2001*.
- "La protección penal de las patentes e innovaciones tecnológicas", de *José Manuel PAREDES CASTAÑÓN, Mc Graw Hill, 2001.*
- "Delincuencia Informática y Fraudes Informáticos" *de Enrique ROVIRA DEL CANTO. Granada, 2002.*
- "Análisis jurídico-penal de la publicidad engañosa en Internet", *de María del Valle SIERRA LÓPEZ, Tirant lo blanch, 2003.*
- *"Infracciones patrimoniales por medios informáticos y contra la información, como bien económico",* de *Eduardo de URBANO CASTRILLO* , en "Delitos contra y a través de las nuevas tecnologías, ¿Cómo reducir su impunidad?.CGPJ, 2006
- *"El documento electrónico: aspectos procesales", de Eduardo de URBANO CASTRILLO* , en "Internet y Derecho Penal", CGPJ 2001.
