LA CRIMINALIDAD EN INTERNET

Francisco Javier Iglesias Carballo
Abogado. Doctorando por el Departamento de Derecho Penal y Estudios Penales de la Universidad de Valladolid

"Internet es la culminación histórica de un proceso global de desarrollo del pensamiento humano.
Es el tejido neuronal de la conciencia colectiva de la humanidad."

Carlos A. Sánchez Almeida (Abogado)

SUMARIO:

1.- INTRODUCCIÓN
2.- LA DELINCUENCIA EN LA RED
2.1.- Generalidades
2.2.- Delitos tradicionalmente denominados informáticos
2.3.- Delitos convencionales
2.4.- El Código Penal de 1995
3.- LOS DAÑOS INFORMÁTICOS.
3.1.- Los Hackers
3.2.- Los daños informáticos en el Derecho penal europeo
3.3.- Los daños informáticos en el Derecho Penal español
3.3.1.- Tipo objetivo
3.3.2.- Tipo subjetivo
4.- LA ESTAFA INFORMATICA
5.- DELITOS CONTRA LA PROPIEDAD INTELECTUAL
6.- DELITOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES.
6.1.- La intimidad y las nuevas tecnologías en el Código Penal.
6.2.- REVELACION DE SECRETOS DE PARTICULARES COMETIDA POR FUNCIONARIO PUBLICO. ARTICULO 198 DEL CODIGO PENAL.
6.2.1.- Tipo objetivo
6.2.2.- Tipo subjetivo
6.3.- REVELACION DE SECRETOS DE EMPRESA. ART. 278 DEL C. PENAL
6.3.1.- Tipo objetivo
6.3.2.- Tipo subjetivo
7.- LOS DELITOS CONTRA LA PROPIEDAD INDUSTRIAL
8.- LA APOLOGIA DEL DELITO EN INTERNET
9.- LA PORNOGRAFIA INFANTIL

1.- INTRODUCCIÓN

El objeto del presente estudio, es el análisis de los diferentes tipos penales que pueden tener cabida en las nuevas tecnologías en concreto vía INTERNET.

Internet (International Network of Computers) se presenta como un paso decisivo en el avance de los sistemas de información y comunicación a escala planetaria. Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más

importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia.

En el ciberespacio no existen fronteras, distancias ni autoridad centralizada. Su conquista se ha convertido en meta obligada para quien desee sentirse miembro de la sociedad informática y es en la actualidad uno de los puntos de encuentro para el ocio y el negocio que cuenta con mayores perspectivas de futuro.

No obstante el ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. A las reconocidas ventajas que el uso de la red supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Así pues, junto con esas incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud. No es lícito, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías. Desde hace tres décadas, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre esos peligros, y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido. Es cierto que España, aun siendo una sociedad avanzada, dista de los países con tecnología punta. De ahí que, entre nosotros, se juzgara mayoritariamente como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad.

Como la mayoría de las grandes conquistas científicas y tecnológicas que registra la historia, Internet es una realidad ambivalente. Renunciar a sus logros sería hoy una pretensión imposible, porque se trata de un avance irrenunciable y un signo del progreso de nuestro tiempo. Pero ello no debe conducir a aceptar pasivamente o a claudicar ante los riesgos de «abordaje» criminal que amenazan la navegación por el ciberespacio.[1]

2.- LA DELINCUENCIA EN LA RED

2.1.- Generalidades

Hay personas que consideran que los delitos informáticos, como tales, no existen. Argumentan que tan sólo son delitos normales que en lo único que se pueden diferenciar, de otro delito cualquiera, son en las herramientas empleadas o en los objetos sobre los que se producen.

[1] PEREZ LUÑO, ANTONIO-ENRIQUE.- La Ley 1997-2.

Entendemos que ésta es una visión demasiado limitada de la realidad: Esto puede ser así si pensamos tan solo en delitos del tipo de un apunte informático falso en un banco o del robo de una cantidad de dinero gracias a la utilización ilícita de una tarjeta de crédito.

Pero existen muchos otros delitos que difícilmente podemos tipificar con las leyes actuales y que estas rápidamente se tendrán que adaptar o redactar acorde a los nuevos tiempos (como ha hecho nuestro Código Penal), que impone el uso de las tecnologías de la información. ¿Porqué, sinó, se habla constantemente de lagunas o de falta de regulación si son los mismos delitos de siempre?.

Un ejemplo clarificador es lo que ocurrió ya con el famoso gusano de Internet (programa informático similar a un virus cuyo estudio se abordará más adelante), que lanzó Robert Morris Jr. en Noviembre de 1.988 y que acabó bloqueando más de 6.000 ordenadores: De no existir en ese momento el Acta sobre Fraude y Abuso Informático en Estados Unidos, es más que dudoso que se le hubiese podido juzgar.

Hay que recordar también que las compañías de seguros, de varios países, ofrecen cobertura concreta contra este tipo de delitos. Sólo en Estados Unidos se calcula que se generan perjuicios económicos, por los delitos informáticos, que superan los 10.000 millones de dólares o más de 5.000 millones de libras esterlinas en el Reino Unido.

También hay que recordar que hasta la propia Dirección General de Policía en España, al igual que muchos otros países, ha tenido que crear un Grupo dedicado en exclusiva a los delitos informáticos.

Casi el 90% de los delitos informáticos que investiga el FBI tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos.

La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común. Es decir, hay que unificar criterios: difícil será actuar contra un delito que sí lo es en un país y no en otro. En este sentido está trabajando, por ejemplo, la Unión Europea.

Es cierto, de todas formas, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio. Lo que ocurre es que no sólo es eso.

Además el avance que está sufriendo Internet en número de usuarios, que parece que vaya a colapsarse en cualquier momento, y en broma se hable ya del ciberdespacio, hace que haya que actuar rápidamente ante los posibles delitos que puedan cometerse a través de ella: con el aumento de la ciberpoblación, aumentan los posibles delincuentes y los posibles objetivos.

Muchas empresas que en un principio no querían conectarse a Internet, precisamente por los posibles problemas de seguridad, ahora no quieren quedarse atrás, ya que se ha convertido en

una cuestión o de pura necesidad o de imagen, y ahora se conectan a marchas forzadas, lo que hace que muchas no tomen las precauciones necesarias y se conviertan automáticamente en jugosos y fáciles objetivos.

Internet no estaba pensada y desarrollada para lo que está ocurriendo: su propio diseño no está basado sobre protocolos hiper-seguros y, tan es así, que hoy día se estima que no existe un sólo servidor en el mundo que no haya sufrido un ataque contra su seguridad por parte de hackers y crackers., cuyo estudio abordaremos más adelante.

Desde el punto de vista de la seguridad también es preocupante el uso de la criptología (cifrado) por parte de los delincuentes, tanto para ocultar sus mensajes haciéndolos ininteligibles, como para ocultar sus propios movimientos en un sistema informático, haciendo que incluso aunque sean detectados no se pueda saber exactamente que es lo que estaban haciendo, al estar encriptados los archivos descubiertos. En este sentido, actualmente es muy inquietante la utilización de cripto-virus (programas con código vírico encriptados).[2]

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar esos malos usos en la red de redes Internet y el objetivo es localizar las distorsiones más habituales que se producen y resumir los argumentos que se han dado a favor de una legislación que regule el uso de la red.

[2] http:///www.ctv.es/USER/mpg/delitos.html

Artículos y conferencias: "Delito informático, fraude informático y legislación penal en Argentina", por el Dr. Miguel del Castillo. (Fundación Veraz). "Los delitos informáticos", por Jorge Lara Rivera. "Fraude en instrumentos de pago. Nuevas modalidades y su impacto en la actividad bancaria", por el Sr. Richard Espinoza de *Mastercard*. (Fundación Veraz). "Fraude en instrumentos de pago", por el Sr. Alberto España de *Visa*. (Fundación Veraz). "La nueva regulación penal de los delitos informáticos", por Josep Padró y Silvia Cabrera Vilaplana.
Debate en Derecho-es
The Computer Crime and Investigation Center
The Computer Law Resource
Comunicación de la Unión Europea sobre contenido perjudicial e ilegal en Internet.
CopNet Completa información sobre las actividades de esta *policía en la red*.
The Digital Crimes Investigation Network Dedicados a investigar y denunciar los delitos cometidos utilizando tecnología digital.

Los partidarios de la regulación se apoyan en la tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados.

Ello no obstante, la propia Organización de las Naciones Unidas ha calificado diversas actividades como delitos informáticos, con la reserva propia de este tipo de declaraciones efectuadas por las organizaciones internacionales, en el sentido de su escasa o nula vinculación respecto a las legislaciones de los países miembros. En este sentido se describen genéricamente diversas actividades delictivas en este campo.[3]

---

[3] Universidad Autónoma de Sinaloa. www.tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm

DELITOS INFORMATICOS RECONOCIDOS POR LA ONU

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

La manipulación de programas: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática : Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas:

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

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

Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: Virus Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede

En este sentido, y teniendo en cuenta la empírica delictiva en el campo informático y más concretamente en el seno de INTERNET, podemos clasificar los tipos del siguiente modo:

regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. Bomba lógica o cronológica Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Acceso no autorizado a servicios y sistemas informáticos: Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. Piratas informáticos o hackers El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

2.2.- Delitos tradicionalmente denominados informáticos

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos en el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos de ciberespacio como un mundo virtual distinto a la vida real, el delito informático es aquel que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información

Dentro de este tipo de delitos o infracciones se podrían destacar:

Acceso no autorizado: El uso ilegítimo de password y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, demás actos de sabotaje informático.

Infracción de los derechos de autor: En este punto, tal y como veremos más adelante, la interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

Infracción del copyright de bases de datos:. No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan “downloads” (copiar diferentes programas a través de la red) de los ficheros contenidos en el sistema, pero prohibe el replicado de las bases de datos o la copia masiva de la información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y del animus defraudandi existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos:. Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al

empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

2.3.- Delitos convencionales

Por otro lado podríamos hacer referencia a los ***delitos convencionales***, los cuales son aquellos que tradicionalmente se han venido dando en la vida real sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se han reproducido también en el ciberespacio. No obstante, teniendo en cuenta el carácter global de INTERNET, alguna de las conductas reseñadas pueden constituir un delito en unos países y en otros no.

Espionaje: Se han dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, sistemas de fabricación y estrategias industriales que posteriormente han sido aprovechadas en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: La existencia de mensajes que ocultan la identidad del remitente, convirtiéndolo en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Tanto el FBI como el Fiscal General de los EEUU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con sus cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. El notable avance de las técnicas de encriptación permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales.

Otros delitos:. Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas,

propaganda de grupos extremistas, blanqueo de dinero (*) y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

2.4.- El Código Penal de 1995

En nuestro ordenamiento jurídico, el Código Penal de 1995, contiene muchas referencias a los delitos informáticos y a los derivados del uso de las telecomunicaciones, entre las que podemos destacar las siguientes:

1.- Delitos contra la intimidad y el secreto de las comunicaciones.

Dentro de esta categoría de delitos hay que distinguir entre la interceptación de correo electrónico y la usurpación y cesión de datos reservados de carácter personal.

a) Interceptación de correo electrónico.

El artículo 197 del CP extiende al ámbito de aplicación de este delito a las siguientes conductas:

.- Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.

.- Interceptación de las telecomunicaciones, en las mismas condiciones.

.- Utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos.

Estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir sus secretos o vulnerar su intimidad. La pena que se establece es de prisión, de uno a cuatro años y multa de doce a veinticuatro meses.

El Código Penal anterior no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de la persona o para violar, acceder y descubrir sus secretos.

b) Usurpación y cesión de datos reservados de carácter personal.

También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir, o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

El art. 197.2 castiga con prisión de 1 a 4 años para el caso de acceso, utilización, etc. Y de 2 a 5 años si los datos se difunden, revelan o ceden a terceros. Cuando dichos actos afectan 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.

Esta inclusión de los datos personales en el Código Penal supone una importante innovación respecto a la regulación anterior.

2.- Estafas electrónicas.

El nuevo CP introduce el concepto de estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina.

El artículo 248 y ss establecen una pena de prisión de 6 meses a 4 años para los reos del delito de estafa, pudiendo llegar a 6 años si el perjuicio causado reviste especial gravedad.

3.- Infracción de los derechos de propiedad intelectual.

El artículo 270 del nuevo CP establece la pena de prisión de 6 meses a 2 años e incluye en la categoría de los delitos contra la propiedad intelectual la fabricación, puesta en circulación, y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Respecto a los delitos contra la propiedad intelectual, con la proliferación de las obras multimedia y el uso de la red, este tipo se aplicará no sólo a los programas de ordenador, sino también a los archivos con imágenes, gráficos, sonido, vídeo, texto, animación etc. Que incorporan las webs y las bases de datos accesibles a través de INTERNET.

4.- Delito de daños.

En el delito de daños se contemplan los supuestos de destrucción, alteración, inutilización o cualquier otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.

El artículo 264.2 establece la pena de prisión, de 1 a 3 años en el caso de daños informáticos.

5.- Difusión y exhibición de material pornográfico a menores.

El artículo 186 tipifica como delito la conducta consistente en la difusión, venta o exhibición entre menores de edad o incapaces, de material pornográfico.

Dicha exhibición o difusión puede efectuarse mediante cualquier medio directo, por lo que entendemos incluida en este supuesto la difusión a través de INTERNET mediante correo electrónico dirigido a menores de edad, o la exhibición a través de una web o una base de datos sin tomar las precauciones oportunas para impedir el acceso a menores.

6.- Pornografía infantil.

El artículo 189 establece que el que utilizare a un menor de edad o a un incapaz con fines exhibicionistas o pornográficos será castigado con la pena de prisión de uno a tres años.

Tal modalidad delictiva, evidentemente tiene fácil comisión a través de la red.

7.- Difusión de mensajes injuriosos o calumniosos.

El artículo 211 establece que los delitos de calumnia e injuria se reputarán hechas con publicidad cuando se propaguen por medio de imprenta, la radiodifusión o cualquier otro medio de eficacia semejante.

Puede incluirse perfectamente en este supuesto la difusión de mensajes injuriosos o calumniosos a través de Internet.

Las penas establecidas pueden llegar a los 2 años de prisión en el caso de la calumnia, y multa de hasta 14 meses en el caso de la injuria.

El artículo 212 establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria.

A nivel jurisprudencial, citaremos una sentencia de la Audiencia Provincial de Valladolid de 19 de Octubre de 1999, que aborda el tema de los mensajes injuriosos a través del correo y que reproducimos íntegramente en nota al final [4]

---

[4] RECURSO DE APELACION NUM. 1103/99 JUICIO DE FALTAS NUM. 93/99 JUZGADO DE INSTRUCCION NUM. 4 DE VALLADOLID

S E N T E N C I A NUM. 811/99

En la ciudad de Valladolid, a diecinueve de Octubre de mil novecientos noventa y nueve.

El Ilmo Sr. Don JOSE ANTONIO SAN MILLAN MARTIN, Magistrado de la Sección Segunda de la Audiencia Provincial de Valladolid, ha visto en grado de apelación, sin celebración de vista pública, el presente procedimiento penal de apelación del juicio de faltas expresado, seguido contra Jesús G.P., Antonio A.R. y µngel V.M., defendidos por la Letrada Doña Francisca F.C., siendo partes en esta instancia como apelantes los citados acusados y como apelado Miguel T.M., defendido por la Letrada Doña Doris B.H.

ANTECEDENTES DE HECHO

PRIMERO.- El Juez de Instrucción núm. 4 de Valladolid, con fecha 18-05-99 dictó sentencia en el Juicio de Faltas del que dimana este recurso, en la que se declararon como hechos probados los siguientes:

"Primero y énico: Se declara probado, que el día 20.10.1998, en las páginas Webs del sistema informático de la Universidad de Valladolid y emitido desde la dirección de correo electrónico de la sección sindical de UGT de esta Universidad, por indicación de tal dirección precedida del nombre Jesús G.P. y dirigida a Fernando C., con la mención del asunto (ESTAFA Y VERGÜENZA), apareció un texto en el que se refiere a una persona, sin mencionar nombres a quien se califica de que no respeta a nada, ni a nadie, insulta a todo el mundo, agredió a un compañero de trabajo, y se le llama "bestia", "gandul", "desaparece de su puesto de trabajo virtual para ocupar su puesto de trabajo real en las barras de los bares"; y se concluye afirmando "que a parte de la otra bestia retenida en Londres hay otros individuos que gozan también de inmunidad, en este caso seguramente por otros motivos", dándose referencias de tal persona de que es trabajador de la Universidad con un cargo de representación sindical y que ha sido sometido a un expediente informativo por supuesta agresión a un compañero de trabajo.

El texto citado termina con la expresión Jesús G.P. y se acredita por la testifical practicada en el acto del Juicio, que el denunciado de tal nombre los puso al menos en dos tablones de anuncios de distintas

dependencias de la Universidad, y en ningún momento negó su autoría, ni publicó nota desautorizando la presunta utilización de su nombre y el contenido del texto.

Asimismo se prueba que el día 19 de Noviembre en el mismo sistema informático de la Universidad y desde la dirección del correo electrónico correspondiente a µngel V., se emitió bajo la denominación "E.P." y dirigido al Grupo N.G. otro texto del citado µngel V. con la indicación final de su nombre completo del centro de emisión y de las señas del mismo, en el que recordando la existencia de unas elecciones sindicales se refiere a la aparición de una persona muy concreta pero sin decir nombre a la que se imputa que ve enemigos por todos los lados, ataca a todos los que no les rían las gracias, llamando fascistas a unos y a otros e insultando y provocando agresiones, para continuar afirmando en relación a esta persona que fue designado para el comite aunque tal designación no ha dado frutos más que para él, y que volverá a llevar su campaña tradicional diciendo: "esto está lleno de corruptos, fascistas e Hijo de p...; este es un facha, este un corrupto y aquel un hijo de p...",.

Se afirma que la persona a la que se contrae el contenido del texto, que su plan es insultar y luego no hacer nada y que no vendría mal un cursillo urgente de defensa personal. Como dato identificativo indirecto de la persona ha de destacarse que en el texto se afirma, que trabaja en mantenimiento, que es miembro del comité de empresa y que se propone de nuevo concurrir a las elecciones. No consta que el denunciado µngel V., que conoció el texto en su integridad emitido desde su dirección de correo electrónico y usando su nombre sacara nota alguna por dicho medio u otro, negando la autoría del texto, no desvinculándose y rechazando su contenido.

Asimismo se prueba que el día 20 de Noviembre de 1998, desde la dirección del correo electrónico de Antonio A.R., con expresión de su nombre y bajo la referencia asunto E.P., se edita texto dirigido al Grupo de N.G., en el que se comenta el mensaje de µngel V. del día anterior y en el que se afirma "tu crees que ese individuo tiene alguna idea exponible y defendible en público" y más adelante en relación a la recomendación de que cuelgue los guantes, se afirma en este último texto "de boxeo serán, claro esta, porque los de seguridad no se los ha puesto en la vida", y cuando se afirma en el texto que se comenta (algo nuevo "Trabaja un poco") se afirma "INEDITO, MILAGROS, INAUDITO, EL QUINTO MISTERIO DE FÁTIMA....". El último de los texto concluye con la mención de Antonio A.R. y una expresión gráfico que ha sido reconocida por el mencionado denunciado como muy parecida a la que ordinariamente utiliza, no constando que haya emitido nota alguna en relación de este texto negando la autoría del mismo o mostrando su conformidad con el contenido.

Se acredita igualmente en el acto del Juicio que el denunciante trabajaba en el servicio de Mantenimiento, con categoría de técnico especialista, grupo tercero, de la Universidad de Valladolid, y ha sido sujeto de un expediente disciplinario por el Rectorado de la Universidad, resulto el 20 de Enero de 1999, en el sentido de imponer al denunciado Miguel T.M. la suspensión de empleo y sueldo de dos días, en relación a insultos y agresión causados en la persona de Julio L.C. No se acredita que pudiera existir otra persona en la Universidad de Valladolid que no fuera el denunciante y a quien pudieran venir referidas las expresiones y circunstancias reflejadas en los textos preferentemente mencionadas. También se acredita por la prueba testifical practicada, que aunque no es imposible técnicamente, sería de gran dificultad la utilización y la circulación por terceros de las direcciones del correo electrónico correspondientes a los denunciados y la utilización de sus claves de acceso.

Dado que no se puede garantizar la seguridad al 100 por 100 en el manejo de cuentas informáticas. Por último, se acredita que en el diario N.C., correspondiente al día 20 de Noviembre de 1998, la denunciada Carmen R. publicó un artículo "La Universidad investiga a un miembro del comité de empresa por agredir a un superior" en el que se da cuenta de la apertura de expediente disciplinario contra el denunciante Miguel T. y del debate provocado por el texto emitido desde la sección sindical de UGT en las páginas Wed del correo electrónico de la Universidad de Valladolid, recogiendo entrecomillados diversos párrafos textualmente transcritos de los textos anteriormente referidos, sin que se falte en absoluto a la verdad o se contenga dato alguno erróneo en la información periodística facilitada".

SEGUNDO.- La expresada sentencia, estimando que los hechos declarados probados eran constitutivos de Falta contiene el siguiente Fallo:

"Que debo condenar y condeno a Jesús G.P., Antonio A.R. y µngel V.M., como autores cada uno de ellos de una Falta de Injurias, ya calificada, a la pena de veinte días Multa a razón de 1.000 pesetas cuota día para cada uno de ellos, con arresto carcelario sustitutorio en caso de impago de un día por cada dos cuotas no abonadas, y al abono de las costas del presente Juicio por terceras partes.

Debiendo Absolver y absuelvo a la también denunciada Carmen R. de la Falta que venía siendo acusada".

TERCERO.- Notificada la mencionada sentencia, contra la misma se formalizó recurso de apelación por Jesús G.P., Antonio A.R. y µngel V.M., que fue admitido en ambos efectos, y practicadas las diligencias oportunas, fueron elevadas las actuaciones a este Tribunal, donde se registraron, se formó el rollo de Sala y se turnaron de ponencia.

No habiéndose propuesto diligencias probatorias y al estimarse innecesaria la celebración de vista para la correcta formación de una convicción fundada, quedaron los autos vistos para sentencia.

CUARTO.- Como fundamentos de impugnación de la sentencia se alegaron sustancialmente los siguientes:

- Error en la apreciación de las pruebas.

- Infracción de precepto legal o constitucional. (Art. 27, 28, 208, 620 y 620.2, del Código Penal y 24 Constitución).

HECHOS PROBADOS

Se aceptan, en lo sustancial, los hechos que se declaran probados en la sentencia de instancia.

FUNDAMENTOS DE DERECHO

PRIMERO.- El recurso de apelación promovido frente a la sentencia de fecha de 18-05-99 del Juzgado de Instrucción núm. 4, de los de Valladolid, debe alcanzar favorable acogida, pues, de un análisis objetivo de la prueba practicada en el acto del juicio, puede apreciarse un error valorativo, por parte del Juzgador de Instancia, que ha determinado una Sentencia de signo condenatoria, que finalmente, infringiría el art. 24 de nuestra Constitución, al vulnerarse el principio constitucional de presunción de inocencia. Efectivamente, aun cuando puede constatarse la existencia de indicios, en los acusados, que pudieran producir sospechas sobre su participación en los hechos, unas notas difundidas en el servicio NEWS de la Universidad de Valladolid (Internet) atribuidas supuestamente la del 30 de Octubre de 1998 a Jesús G.P., la del 19 de Noviembre de 1998 a µngel V.M. y la del 20 de Noviembre de 1998 a Antonio A.R.; de otra parte se denuncia la publicación de un artículo en el Diario N.C., atribuida a la periodista Carmen R. y por último se denuncian unas supuestas amenazas telefónicas.

Hay que concluir, que tales indicios, no resultan unívocos (dirigidos a unos mismos hechos nucleares sobre los que recae la labor acreditativa, ante la inexistencia de prueba directa) ni excluyentes de la posibilidad de participación en los hechos (sobre cuya punibilidad y existencia real, no hay cuestión en las actuaciones) de otras terceras personas. Por lo que surge, la fundada "duda" respecto de la autoría de los condenados, lo que exige la aplicación del principio constitucional de "in dubio pro reo". Los denunciados, han venido sosteniendo en todo momento su no autoría, en términos absolutos, sobre la comisión de los hechos, incluso, su no conocimiento de los mismos, hasta ya momentos bien tardíos. La accesibilidad a la página de correo electrónico y la enorme posibilidad de acceso a la misma de cualesquiera otras personas, además de los denunciados, debe darse por acreditada en autos, merced a la documental aportada en el acto del juicio (nada sospechosa), por expertos en temas informáticos, además, dentro del ámbito de la Universidad, lugar de desarrollo de los hechos.

Lo que muy bien puede concluirse, en que cualquier persona, con unos mínimos conocimientos de operatividad en ordenadores con conexión a Internet, de configuración de correo electrónico (de muy amplia divulgación pública), con el simple conocimiento de la dirección electrónica de una segunda persona y simplemente por su conexión a Internet de la Universidad, tiene aptitud para realizar notas como las tomadas en consideración. (En la Mensajería de la Universidad, no se precisa de verificación o contraseña). Las cuentas abiertas, propiedad sobre direcciones de correo electrónico, desde la que se pretende emitidas las notas, con implicación de los acusados, resulta ser de la Sección Sindical de UGT de la Universidad, otra del trabajador de ese mismo Centro, el acusado Antonio A.R., y la tercera a la E.T.S. de Ingenieros de Telecomunicación de la misma Universidad; en todo caso, todas de cuasi naturaleza pública y amplio acceso a su uso.

El único elemento probatorio de mayor consistencia, correspondería a las testificales verificadas sobre el acusado Jesús G.P., cuando refieren haber sido visto, estampando en el tablón de anuncios alguna de esas notas de referencia en autos, pero aun prescindiendo de las imprecisiones sobre el concreto momento en que afirman haber visto al acusado, fijar tal nota, y su correspondencia con las portadoras de los mensajes injuriosos, ello, deja sin acreditarnos, la auténtica autoría de la confección de la misma, acreditando solo el acto de exhibirlas en un tablón de anuncios, sea cual fuera la fuente de su obtención. Por todo lo cual, se está en el caso de revocar la Sentencia condenatoria dictada, declarándose en su lugar, la libre absolución de los apelantes, de la falta de injurias por la que fueran condenados.

Vistos los preceptos legales y demás de general y pertinente aplicación,

En el caso de Internet, la responsabilidad civil solidaria alcanzaría al propietario del servidor en el que se publicó la información constitutiva de delito, aunque debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de información contenida en un servidor no es comparable al de una revista, un periódico o un programa de TV o radio.

En este sentido cabe recordar la tesis que asimila al propietario de un servidor al librero, en contraposición con los que lo asimilan a un editor. La primera teoría es partidaria de liberar de responsabilidad civil al propietario de un servidor, debido a la imposibilidad de controlar toda la información que es depositada en el mismo por los usuarios.

8.- Publicidad engañosa en Internet.

El uso de INTERNET con fines publicitarios, hace que se trasladen con esos mismos fines eslogans y mensajes que se difunden en la vida real. Ello hace posible la aplicación de la ley a las infracciones que se produzcan en el ciberespacio y que puedan causar un perjuicio grave a los consumidores.

En este sentido el artículo 282 castiga con la pena de prisión de seis meses a un año a los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

9.- Robo.

El artículo 239, considera llaves falsas las tarjetas magnéticas o perforadas así como los mandos o instrumentos de apertura a distancia, considerando por lo tanto delito de robo la utilización de estos elementos, el descubrimiento de claves y la inutilización de sistemas específicos de alarma o guarda con el fin de apoderarse de cosas muebles ajenas.

10.- Revelación de secretos contenidos en documentos o soportes informáticos.

F A L L O

ESTIMANDO el recurso de apelación interpuesto por JESéS G.P., ANTONIO A.R. Y µNGEL V.M., contra la sentencia de fecha 18-05-99 dictada por el Juzgado de Instrucción núm. 4 de Valladolid, en el Juicio de Faltas núm. 93/99, debo revocar la referida resolución recurrida. Con expresa declaración de oficio, de las costas procesales causadas en este recurso, y de las de primera instancia. Declarandose en su lugar la libre absolución de los acusados de la Falta de injurias por la que resultaron condenados.

Remítase testimonio de la presente al Juzgado de procedencia, junto con los autos, para su notificación y cumplimiento, y una vez se reciba su acuse archívese el presente, previa nota en los libros.

Así por esta sentencia, lo acuerdo, mando y firmo.

El artículo 278 establece una pena de 2 a 4 años para el que, con el fin de descubrir un secreto, se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo.

Si los secretos descubiertos se revelasen, difundieren o cedieren a terceros, la pena llegará a los 5 años de prisión.

11.- Falsedad en documento electrónico.

Los artículos 390 y siguientes castigan con la pena de prisión de hasta seis años las alteraciones, simulaciones y demás falsedades cometidas en documentos públicos.

Los artículos 395 y 396 se refieren a las falsedades cometidas en documentos privados, pudiendo alcanzar la pena de prisión hasta dos años. También se castiga la utilización de un documento falso para perjudicar a un tercero.

El artículo 26 define como documento cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

Entendemos que quedaría incluído en el concepto de documento los mensajes estáticos, compuesto por información almacenada en un sistema informático después de haber sido remitida o recibida a través de la red, pero surgen dudas sobre la naturaleza documental del mensaje que está circulando.

12.- Fabricación o tenencia de útiles e instrumentos específicamente destinados a la comisión de delitos.

El artículo 400 introduce el delito consistente en la fabricación o tenencia de útiles, materiales, instrumentos, programas de ordenador o aparatos destinados específicamente a la comisión de estos delitos, se castigarán con las penas señaladas para los autores. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo similar.

13.- Sustracción, destrucción, inutilización u ocultación de documentos electrónicos por parte del funcionario público cuya custodia le esté encomendada por razón de su cargo[5].

---

[5] En el nuevo Código Penal español (aprobado por Ley-Orgánica 10/1995, de 23 de Noviembre / BOE número 281, de 24 de Noviembre de 1.995) hay varios artículos íntimamente relacionados con el tema que estamos tratando.

Son los siguientes:

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.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200

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.

Artículo 201

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211 (Nota: Tanto este artículo como el siguiente presentan un bonito debate. ¿Se pueden considerar que son de eficacia semejante Internet y los medios de comunicación tradicionales? ¿Son responsables los administradores de sistema o las empresas propietarias de los servidores?).

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

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

1º.- Escalamiento.

2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.

4º.- Uso de llaves falsas.

5º.- Inutilización de sistemas específicos de alarma o guarda.

Artículo 239

Se considerarán llaves falsas:

1º.- Las ganzúas u otros instrumentos análogos.

2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.

3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

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.

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:

1º.- Valiéndose de mecanismos instalados para realizar la defraudación.

2º.- Alterando maliciosamente las indicaciones o aparatos contadores.

3º.- 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.

Artículo 263

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264

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 concurriera alguno de los supuestos siguientes:

Hecha esta genérica descripción de los delitos informáticos se procede a analizar más detalladamente los tipos que desde el punto de vista de este modesto doctorando merecen mayor atención. En concreto, los daños informáticos con especial detenimiento en la figura de los hackers, las estafas, delitos contra la propiedad intelectual e industrial, los delitos contra la intimidad y revelación de secretos, la apología del delito y la pornografía infantil. Todos ellos por

---

1º.- 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 pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

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

3º.- Que se empleen sustancias venenosas o corrosivas.

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

5º.- 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.

Artículo 270

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte 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 intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

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

Artículo 278

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o elctrónicos, soportes informáticos u otros objetos que se refieran al micmo, 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.

Artículo 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación.

lo que se refiere a su comisión a través de la red, y ello teniendo en cuenta la posibilidad de perpretación a través de otros medios, sobre todo por lo que respecta a los daños informáticos.

3.- LOS DAÑOS INFORMÁTICOS.

3.1.- Los Hackers

El nuevo Código Penal español incorpora como figura cualificada o agravada de daños en el Título XIII, Capítulo II, art. 264.2, denominado sabotaje informático.

Siguiendo a la profesora **Andrés Domínguez**, diremos que el sabotaje informático consiste en la destrucción o deterioro, tanto del soporte físico como del lógico de un ordenador, con el fin inmediato de imposibilitar la utilización de la información almacenada o procesada.

Ninguna particularidad ofrecen los comportamientos lesivos referidos al soporte físico, dentro de los cuales se pueden incluir los atentados al Hardware propiamente dicho y a los edificios o locales que los albergan, ya sean aquéllos el objetivo inmediato o la destrucción de la información procesada. Tipos delictivos que se cometen por acción física directa, manteniéndose al margen de los cometidos a través de la red.

Distinta es la situación cuando los ataques se dirigen a los elementos lógicos, es decir, órdenes, ideas que se registran en un medio al que se accede electrónicamente, y que pueden ser definidos como un flujo electromagnético; el hecho de que la acción recaiga sobre los elementos lógicos del sistema informático es lo que verdaderamente caracteriza, y de forma peculiar, al sabotaje informático.

Estos ataques a los elementos lógicos pueden llevarse a cabo bien a través de medios físicos, bien por procedimientos propiamente informáticos, siendo estos últimos los más sofisticados, eficaces y difíciles de detectar y los que nos interesan a los efectos del presente estudio y los que plantean multitud de problemas desde el punto de vista penal en orden a autoría, consumación, dolo...

Los procedimientos de destrucción de elementos lógicos de un sistema informático más conocidos son:

a) Crash programs o programas de destrucción progresiva. Con ellos se pueden borrar un gran número de datos en un corto período de tiempo.

b) Bombas lógicas de actuación retardada o Time Bombs. La destrucción de los ficheros se produce tras un lapso de tiempo en virtud de indicaciones precisas como la presencia o ausencia de un dato, de una hora, de un código, de un nombre. El problema esencial es que la destrucción de los ficheros se produce de forma autónoma por el propio sistema informático . Una modalidad de esta clase de sabotaje surge en aquellos supuestos en los que la destrucción ha sido programada por el mismo propietario del Software.

c) Superzapping. Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador.

d) Cancer rutine. Consiste en introducir una serie de órdenes que provocan su propia reproducción en otros programas arbitrariamente escogidos; pueden ser detectadas y sacadas, pero si permanece alguna el cáncer sigue extendiéndose.

e) Virus programs o virus. Son programas que pueden multiplicarse y contaminar otros programas que están en el disco duro y los programas y datos de otras empresas en el transcurso de una conexión. Puede destruir no sólo rutinas y datos, sino que combinado con bombas lógicas activado al mismo tiempo o posteriormente infecta el sistema completo e incluso las copias de seguridad. Provoca una mayor lentitud en la ejecución de los programas, y el bloqueo del funcionamiento de la pantalla o la aparición en ésta de signos extraños, la desaparición de informaciones del disco duro... . Los virus son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección. Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente EXE y COM, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado, y así sucesivamente. Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero. Se estima que en la actualidad el número de virus asciende a más de 7.000 y su número crece considerablemente cada día. Un ejemplo de los últimos virus más dañinos son el famoso *I love you,* y muy recientemente el denominado *Enmanuelle.* Ambos utilizan como vía de infección el correo electrónico y su repercusión en los equipos informáticos es enormemente nociva.

f) Puertas falsas. Requiere una especial cualificación técnica. Consiste en la producción de interrupciones que hacen los programadores para el chequeo del programa, con lo que se dejan puertas falsas para entrar en él. Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

g) Caballo de Troya. Consiste en introducir en un programa de uso habitual una rutina o conjunto de instrucciones para que dicho programa actúe de forma distinta a la prevista. Para su utilización se requiere una capacitación técnica suficiente, al menos saber programar y tener acceso al programa para poder manipularlo. Es un método difícil de detectar, pero fácil de prevenir. Tiene similitud con las bombas lógicas, aunque generalmente el caballo de Troya se usa para cometer

un fraude y aquéllas como medio de sabotaje p. ej. formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos los crean los programadores, ya sea creando ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

h) System Crosh. Consiste en introducir una orden que provoca el bloqueo del sistema informático.

i) Ataques asincrónicos. Procedimiento complejo que se basa en la forma de funcionar de los sistemas operativos y sus conexiones con los programas de aplicación a los que sirven y soportan en su ejecución. Este es quizá el procedimiento mas complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

j) Los Hackers. Jóvenes fanáticos de la informática con un ordenador, un módem y una gran imaginación que son capaces de acceder a través de una red pública de transmisión de datos al sistema informático de una empresa, institución bancaria... introduciéndose en él[6].

Conviene antes de describir las armas que utilizan los hackers, hacer una breve puntualización por lo que respecta a citados “delincuentes”. A pesar de que con posterioridad denominaremos genéricamente hackers, a las personas que se dedican a sabotear sistemas informáticos de muy diversas formas a través de la red, conviene decir que tal definición tan ámplia es un tanto errónea.

La red ha dado muchos titulares a los periódicos sobre vulneraciones de sistemas, obtención de datos secretos, etc. Y como había que llamarlos de alguna forma se los denomina, en círculos profanos, hackers. Todo esto ha creado en la sociedad una confusión sobre la denominación a estas personas, y se utiliza esta palabra para comportamientos diferentes.

Un **hacker** es una persona muy interesada en el funcionamiento de sistemas operativos; suele tener mucho conocimiento en lenguajes de programación. Además conoce la mayoría de los agujeros de un sistema operativo o de los protocolos de Internet, y los que no conoce los busca, y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor. Se puede decir que los hackers, normalmente se mueven por fines de autorrealización y conocimiento, no suelen provocar daños intencionados en las máquinas, y por regla general

[6] Dra. Ana Cristina Andrés Domínguez. La Ley 1999-1.

comparten su información de forma gratuita y desinteresada. Obviamente la difunden también para que se le reconozcan los méritos de su trabajo, pero eso sucede en todas las actividades humanas. Ello no obstante, en España su actividad por muy "pedagógica" que pueda parecer vulnera el derecho a la intimidad, un derecho fundamental que proclama la Constitución Española de 1978, y otros preceptos de nuestro ordenamiento jurídico;

Por su parte, los **crackers** son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

Pero estas definiciones son demasiado generales para denominar de una u otra forma a una persona, que se introduce en otros sistemas ajenos; deberíamos conocer sus motivos, intenciones, etc.

Un aspecto para diferenciar a un hacker de un cracker puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación, y además en varios lenguajes de programación, mientras que el segundo se basa en programas ya creados que puede adquirir, normalmente, vía Internet. Otro aspecto diferenciador es que el interés de un cracker es destrozar la máquina que hay al otro lado, no es constructivo como un hacker, que trata de "mejorar" la red dando a conocer sus incursiones y los fallos que ha encontrado.

¿Por qué existen los crackers? La existencia de los crackers es muy simple, al igual que en la vida real nos podemos encontrar personas constructivas y otras destructivas, en la red también sucede lo mismo. Además muchos crackers son como mercenarios, es decir, obtienen información restringida de los sistemas a los que entran y luego la venden al mejor postor, o puede ser incluso que haya sido contratado para que busque algo en concreto que interesa a alguien (normalmente empresas que quieren conocer secretos de otras). A estas personas se las suele denominar erróneamente hackers, pero no es así son crackers.

Como se ha dicho antes, los hackers comparten sus descubrimientos con el resto de usuarios de Internet, lo cual hace que se conozcan los fallos de seguridad en las redes, y se ponga remedio a esos fallos, con lo que cada vez conseguimos una red más segura y fiable, esto es lo que los diferencia de los crackers, los cuales sólo tienen un ánimo destructivo, pues venden información, destruyen datos, modifican ficheros, introducen en los programas códigos malignos, que crean problemas en el sistema donde se ejecutan, en definitiva, lo único que hacen es crear problemas en la red.

Hecha tal puntualización, pasamos a exponer las **armas de los hackers.**

A continuación se va a hacer una descripción de las herramientas o métodos que más suelen utilizar los hackers para sus ataques. Pero esta lista esta limitada desde el mismo momento en que se decide crearla, porque la mayoría de los hackers saben programación y se hacen sus

propios programas para entrar a los sistemas, con lo que aquí se tratará de describir los métodos más habituales.

ESCÁNERES

Los escáneres han sido las herramientas más efectivas dentro del hacking, se dice que un escáner tiene más eficacia que miles de passwords.

Un escáner es un sistema que encuentra automáticamente los fallos de seguridad de un sistema remoto, es decir, una persona desde su habitación puede conocer los agujeros de seguridad de un sistema en otro país. Los escáneres son programas que atacan otros ordenadores, almacenando la respuesta que se obtiene, y así una persona puede obtener todo tipo de información de otro sistema, como, por ejemplo, si es posible que un usuario anónimo se registre.

CAZADORES DE CONTRASEÑAS

Un cazador de contraseñas es un programa que desencripta (descifra) las contraseñas o elimina su protección. El funcionamiento es el siguiente: cogemos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización.

HERRAMIENTAS DE DESTRUCCIÓN

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocará el cuelgue del sistema. Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bombs, aplicaciones especiales de negación de servicio, y virus.

Mailbombing: Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario.

Flash bombs:. Cuando nos conectamos a un canal o chats, cada chat tiene su operador que es la autoridad en ese chat, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bombs. Las aplicaciones de flahs bombs que existen atacan de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal.

Aplicaciones de negación de servicio: Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina.

Virus: ya definidos anteriormente.

INGENIERA SOCIAL

Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

RECOGIDA DE BASURA

Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos: el físico y el electrónico. El físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, p ej. el papel donde un operario apuntó su password y que tiró al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc. El electrónico, se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada, p. ej. ficheros de swapping, ficheros borrados recuperables (por ejemplo, undelete), ficheros de spooling de impresora, etc.

SIMULACION DE IDENTIDAD

Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo desconectó y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

SPOOFING

Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña.

SNIFFER

Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de datos, y el sniffer está diseñado para capturar y guardar esos datos y poder analizarlos con posterioridad.

CABALLOS DE TROYA O TROYANOS

SUPERZAPPING

PUERTAS FALSAS

ATAQUES ASINCRONICOS

Todos ellos ya descritos en el apartado anterior[7].

[7] http://www.geocities.com

A título meramente empírico e ilustrativo, citaremos un caso real, publicado en la página http://delitosinformaticos.com/hack/hacking.htm , consistente en el ataque de hackers a Microsoft, accediendo a información vital para la compañía.

Hackers asaltan Microsoft y acceden a información vital para la compañía.

Los sistemas de Microsoft no se han librado del ataque de los temidos hackers. Uno de los secretos mejor guardados del mundo, el código fuente del sistema operativo mas usado, puede haber sido sustraido de las instalaciones que la compañía tiene en Redmond.

La forma en que se produjo fue mediante un correo eléctronico enviado a un empleado de Microsoft que contenía un virus oculto denominado QAZ.Trojan.

Funcionamiento del QAZ.

El virus se adjunta a un e-mail y el descuidado receptor lo abre ajeno a la peligrosidad del mismo. Se instala en el ordenador, renombra el programa notepad.exe como note.com y el virus pasa a llamarse a si mismo notepad.exe. Al ejecutar el notepad.exe (Bloc de Notas) el virus se pone en funcionamiento, extendiéndose por toda la red local y repitiéndose el proceso de infección. A continuación envía las direcciones de las máquinas infectadas mediante un correo al pirata y éste con esa información es capaz de conseguir cierto control sobre los ordenadores infectados, permitiendo acceder a las claves de los usuarios. Esta información se envía mediante un nuevo correo, pudiendo acceder a la red.

Posiblemente mediante el troyano QAZ el hacker pudo acceder al código fuente del windows 2000 y Me, los lectores de correo Outlook y Outlook Express y el paquete Office. Mediante el código fuente podría realizar:

Podría crear un producto similar a Windows, mejorándolo y ofreciéndolo a un menor precio.

Tendría acceso a los errores y fallos del sistema, intentando aprovecharse de ellos.

Vender el código a programadores interesados.

Y por último, intentar extorsionar a la empresa.

El caso, que fue descubierto por los servicios informáticos gracias al escaneo de los correos salientes, donde se detectaron las claves de los empleados. El tiempo en que el intruso estuvo introducido en los ficheros de la compañía se pudo producir hace tres meses, aunque fuentes de la compañía afirman que ha sido desde hace un mes. Lo más grave del caso es que se ha podido acceder a información de los próximos productos que Microsoft espera sacar al mercado.

El hacker empleo el ordenador de un empleado, que trabajaba desde su casa para introducirse en el sistema.

Este acceso al código fuente puede ser considerado como espionaje industrial, cuyo estudio es objeto de otro apartado del presente trabajo.

3.2.- Los daños informáticos en el Derecho penal europeo

Siguiendo nuevamente a la profesora Andrés Domínguez haremos una referencia a la normativa europea en la materia, tanto desde el punto de vista comunitario como de algunos estados miembros para luego estudiar la regulación en nuestro Código Penal.

1. Normativa europea. Regulación penal en los Estados miembros

El Consejo de las Comunidades Europeas adopta el 14 de mayo de 1991 la Directiva 250 sobre protección de programas de ordenador, instando a los Estados miembros a adoptar las disposiciones de derecho interno necesarias para su cumplimiento. En la misma se establece que los programas de ordenador son objeto de protección, mediante derechos de autor, como obras literarias, extendiendo la protección a cualquier forma de expresión de un programa. Los Estados miembros, de conformidad con sus legislaciones nacionales, deben adoptar medidas oportunas para evitar la puesta en circulación de una copia de un programa de ordenador conociendo su origen ilícito, la tenencia con fines comerciales de una copia de un programa de ordenador conociendo o pudiendo suponer su naturaleza ilegítima, así como la puesta en circulación o tenencia con fines comerciales de cualquier medio apto para facilitar la supresión o neutralización de cualquier dispositivo técnico utilizado para la protección de un programa de ordenador.

Si bien esta Directiva se refiere exclusivamente a la protección del Software, a través de los derechos de autor, y no directamente al sabotaje informático, sí sirve para comprobar la preocupación existente en el seno de la Unión Europea por todo lo relativo al mundo informático y su protección. Preocupación que, como veremos a continuación, se manifiesta en la legislación de los distintos Estados miembros.

En efecto, ante estas nuevas formas de delincuencia que supone el sabotaje informático, el legislador penal europeo ha reaccionado optando por la creación de específicos tipos penales, ante la imposibilidad de los ya existentes para abarcar todas las peculiaridades que presenta la delincuencia informática. Estos tipos de nueva creación pueden consistir, a su vez, en un complemento de los ya existentes corrigiendo en la descripción de la acción típica las carencias detectadas en aquellos principalmente en lo referente al objeto material y modalidades de comisión; posibilidad que Romeo Casabona denomina tipos de equivalencia. O bien, en la descripción de conductas normalmente peligrosas para el correcto funcionamiento de los sistemas informáticos y sus componentes.

Los modelos alemán, italiano, portugués, austríaco siguen la primera vía señalada, mientras que el francés se inserta en la segunda. Veamos, a título de ejemplo, alguna de estas regulaciones:

1. Italia. El art. 9 de la Ley de 23 de diciembre de 1993 introduce en el Codice penale el art. 625 bis «Danneggiamento de sistemi informatici o telematici» a continuación del delito de dannegiamento (art. 635) como tipo independiente de éste y no como mera cualificación, aun cuando figura en el mismo título y capítulo (Tít. XIII, Cap. I, Libro II).

La acción consiste en destruir, deteriorar o hacer inservible total o parcialmente un sistema informático ajeno o bien programas, informaciones o datos. La pena a imponer es de reclusión de siete meses a tres años, salvo que el hecho constituya delito más grave.

En el párr. 2.º se prevé la posibilidad de elevar la pena de reclusión de uno a cuatro años si concurren alguna de las circunstancias que agravan el delito de daños (danneggiamento) o el hecho es cometido abusando de la cualidad de trabajador del sistema.

2. Alemania. Los parágrs. 303 a) a 303 b) del StGB recogen los daños al sistema informático. El primero de ellos castiga con pena de prisión de hasta dos años o multa el borrado, la supresión, inutilización o alteración ilegal de datos almacenados o transmitidos de forma electrónica, magnética o de cualquier forma no perceptible inmediatamente; es decir, se castiga el hecho de hacer ilegibles los datos, o impedir el acceso a los mismos por parte de los sujetos autorizados o bien su transformación que menoscaba la utilidad de los mismos.

El parágr. 303 b) contiene una agravación, que eleva la pena de prisión hasta cinco años, consistente en la interferencia en un proceso de daños de esencial importancia para los negocios o empresas o autoridad administrativa; interferencia que puede llevarse a cabo bien a través de la comisión del delito previsto en el parágrafo anterior (borrar, suprimir, alterar o inutilizar datos), bien a través de la destrucción, daño, inutilización o alteración de sistema o fichero de datos. En ambos supuestos la tentativa es punible.

Por último, el parágr. 303 c) recoge el aspecto procesal en orden a la persecución de los citados delitos.

Si bien estos preceptos se encuentran junto al delito de daños a las cosas (Schadebeschädigung) en la misma sección (26. Abachnitt) del StGB, la doctrina distingue ambas figuras claramente.

3. Francia. En el Derecho francés el Code penale recoge los ataques informáticos en un capítulo autónomo e independiente. En efecto, en el Cap. III, Tít. II bajo la rúbrica «Des atteintes aux systémes de traitement automatisé de donnés» los arts. 323.1 a 323.7 recogen diversas posibilidades de ataques a los sistemas informáticos y a los datos, así como una serie de reglas específicas para su represión.

Las incriminaciones específicas se encuentran en los arts. 323.1 a 323.3. El primero castiga con prisión de un año y multa de 100.000 francos el acceso o mantenimiento fraudulento en un sistema de tratamiento automatizado de datos. Se trata de una fórmula amplia que comprende toda técnica de acceso (utilización del código por persona no autorizada, mantenimiento sin

derecho en el sistema...) no siendo necesario que el acceso se encuentre protegido por un dispositivo de seguridad. La pena se eleva a dos años de prisión y multa de 200.000 francos si a consecuencia del acceso o mantenimiento se produce la supresión o modificación de los datos contenidos en el sistema o la alteración del funcionamiento de éste.

El art. 323.2 castiga con prisión de tres años y multa de 300.000 francos el entorpecer o falsear el funcionamiento de un sistema de tratamiento automatizado de datos, siendo indiferente que se falsee el sistema de tratamiento o el de transmisión. El hecho de entorpecer supone paralizar el sistema de forma temporal o definitiva (sabotaje, introducción de virus...); mientras que el acto de falsear consiste en desviar el funcionamiento del sistema, es decir, conducir a resultados distintos de los esperados. En este supuesto no se exige una intención fraudulenta .

El art. 323.3 recoge la denominada piratería informática, castigando con la misma pena que el anterior (prisión de tres años y multa de 300.000 francos) el hecho de introducir fraudulentamente datos en un sistema o suprimir o modificar los ya existentes. Se protegen los datos no el material o el programa.

La tentativa es punible en todos los delitos de ataque al sistema de tratamiento automatizado de datos (art. 323.7). Por último, el art. 323 núms. 4, 5 y 6, establecen, respectivamente, la punición de la asociación de malhechores, la responsabilidad de las personas jurídicas y penas complementarias aplicables a las personas físicas por la comisión de los hechos previstos en los artículos anteriores[8].

3.3.- Los daños informáticos en el Derecho Penal español

El legislador español ha estimado que los ataques al sistema informático constituyen una simple modalidad o subtipo agravado de la figura de daños en cosa ajena. El párr. 2 del art. 264 (Tít. XIII, Cap. IX), donde figura el catálogo de circunstancias que agravan los daños, castiga la destrucción, alteración, inutilización o cualquier otro daño de datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, con pena de prisión de uno a tres años y multa de 12 a 24 meses. Estamos ante una agravación basada en la peculiar naturaleza del objeto material: los elementos lógicos de un sistema informático, cosa incorporal o inmaterial.

La inclusión de los daños informáticos como figura agravada de los daños en cosa ajena supone que ambas comparten elementos o caracteres comunes esenciales, incorporando la primera alguna circunstancia que la cualifica y permite la elevación de la pena a imponer. Sin embargo, un breve análisis de la figura de daños en cosa ajena nos va a permitir afirmar que no es así y que la inclusión del sabotaje informático como mera agravación no es la vía más adecuada para la necesaria protección penal de esta figura.

[8] Dra. Ana Cristina Andrés Domínguez. La Ley 1999-1.

El delito de daños se caracteriza como delito contra el patrimonio, entendido éste en el sentido de la teoría jurídico-económica, como conjunto de valores que pertenecen a una persona bajo la protección del Ordenamiento Jurídico y como conjunto diferenciado de bienes no como universitas iuris, y más concretamente contra la propiedad en su sentido estricto jurídico-privado.

El bien jurídico protegido en los daños en cosa ajena lo constituye el contenido jurídico y económico de la propiedad sobre la integridad material de un objeto, sobre su existencia o permanencia incólume.

El objeto material, la exigencia de corporalidad, constituye, pues, el primer y principal obstáculo para considerar los daños al sistema informático como un subtipo agravado de la figura de daños en cosa ajena.

A este inconveniente hay que añadir el que supone el comportamiento típico de daños. El Código Penal no describe en ningún momento la acción típica, limitándose a prohibir la causación de daños en propiedad ajena. Esta circunstancia ha permitido la discusión doctrinal en torno a si los daños requieren el ataque a la integridad de la cosa ocasionando en ésta un quebranto material o si es suficiente el ataque al valor de uso del objeto sin quebranto material alguno; discusión que se complica habida cuenta de que en el término inutilizar, que junto a los de destruir, deteriorar y dañar se emplea en la descripción de la figura tienen cabida ambas acepciones: el quebranto físico y el funcional.

Siendo coherentes, los daños al sistema informático se apartan del genuino tipo de daños en cuanto al comportamiento típico. Daño físico y funcional y, en consecuencia, daño típico habrá únicamente cuando la alteración o inutilización de los datos y programas, del soporte lógico derive del daño en el soporte físico; pero no cuando la alteración de los daños no afecta a la integridad del Hardware, a su plena capacidad de funcionamiento o al soporte físico de almacenamiento que puede seguir funcionando.

A estas diferencias sustanciales entre el genuino tipo de daños en cosa ajena y los daños informáticos hay que añadir una más: el resultado típico es el daño, el efecto concreto que sobre el objeto material produce la acción llevada a cabo por el autor, con independencia de sus repercusiones en el patrimonio del sujeto. Se trata de un daño físico-funcional y económico: el valor que desaparece o disminuye es el valor económico, directamente convertible en dinero, ínsito en la cosa; la pena se impone en función del valor económico de la cosa dañada no del perjuicio ocasionado que integrará el montante de responsabilidad civil que deriva de todo delito o falta. En los daños al sistema informático, ¿cuál es el valor monetario de los datos alterados o inutilizados?, ¿no se está confundiendo en este caso el valor económico, el daño, del objeto con el perjuicio patrimonial?; ¿rige para el supuesto del art. 264.2 la cuantía de 50.000 pesetas que permite distinguir el delito de la falta?. A estos interrogantes se puede añadir el siguiente: ¿cómo calificar el supuesto de unos jóvenes (Hackers) que por diversión acceden al ordenador de un

acuartelamiento militar y modifican los datos relativos a la previsión de guardias, descanso, etc., de las tropas, sin afectar a ninguna materia de carácter secreto o reservado? ¿Constituye un delito del art. 264.2 o del art. 265: daños a objetos de las F.A.S.? A este respecto citaremos el único supuesto que se ha dado en los Juzgados y Tribunales españoles, denominado ***CASO HISPAHACK***. El Juzgado de lo Penal número dos de Barcelona absolvió a un presunto Hacker de un delito de daños previsto y penado en el artículo 264.2 del Código Penal

Centrándonos en el tema de los hackers, y teniendo en cuenta la sentencia citada, hemos de decir cuales son los elementos del tipo al objeto de poder apreciar la dificultad de aplicación en la práctica forense, pese a la gran labor que están realizando los peritos informáticos, a la hora de informar a los órganos jurisdiccionales[9].

---

[9] www.bufetalmeida.com

CASO !HISPAHACK: LA SENTENCIA

JUZGADO DE LO PENAL NÚM. DOS BARCELONA

En Barcelona, a veintiocho de mayo de mil novecientos noventa y nueve.

El Ilmo. Sr. D JUAN CARLOS LLAVONA CALDERON, Magistrado-Juez del Juzgado de lo Penal nº 2 de los de esta capital, ha visto en juicio oral y publico las presentes actuaciones de Procedimiento Abreviado Nº 130/99-E de la Ley Orgánica 7/1988, de 28 de diciembre, dimanante de Diligencias Previas nº 1206/98 del Juzgado de Instrucción nº 20 de Barcelona, seguidas por un presunto delito de daños contra el acusado JFS en libertad provisional por esta causa, defendido por el Abogado Carlos A. Sánchez Almeida y representado por el Procurador Carlos Pons de Gironella, siendo parte acusadora el Ministerio Fiscal.

ANTECEDENTES DE HECHO

PRIMERO.- Por el Juzgado de Instrucción nº 20 de Barcelona se incoaron Diligencias Previas nº 1206/98, en virtud de atestado instruido por la Unidad de Policia Judicial de la Guardia Civil, habiendo formulado el Ministerio Fiscal escrito de acusación contra JFS, por lo que se acordó la apertura del juicio oral, correspondiendo su conocimiento a este Juzgado, que incoó el Procedimiento Abreviado nº 130/99-E.

SEGUNDO.- El acto del juicio oral se ha celebrado el pasado 26 de mayo, practicándose en el mismo las pruebas siguientes: Interrogatorio del acusado, Testifical de JBT, BVV, los agentes de la Guardia Civil titulares de los carnets nº 26.001.263 y 118.189, AMT y MFB, respectivamente, Pericial a cargo de JIG y PFG, y Documental.

TERCERO.- El Ministerio Fiscal en sus conclusiones definitivas estimó los hechos como constitutivos de un delito de daños, previsto y penado en el art 264-2 del Código Penal, del que era autor el acusado, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, solicitando que se le impusiera la pena de dos años de prisión y multa de dieciocho meses a razón de 1000 pesetas de cuota diaria, con responsabilidad personal subsidiaria de 270 días y costas.

CUARTO.- La defensa del acusado, en su escrito de conclusiones provisionales elevadas a definitivas, manifestó su disconformidad con las conclusiones del Ministerio Fiscal, solicitando su libre absolución.

HECHOS PROBADOS

Así expresamente se declaran, que a las 4,16 horas del día 11 de septiembre de 1997 se produjo un acceso no autorizado a través de Internet en los ordenadores ubicados en las dependencias de la UPC, desde un ordenador situado en el campus de V., en G., de la Universidad de O. denominado "proy6.etsiig.uniovi.es", llegando a obtener los privilegios del administrador del sistema en al menos dieciseis máquinas servidoras e instalando programas "sniffers" destinados a capturar información que circula por la red del sistema, en concreto identificadores y claves de acceso de otros usuarios, enviando los datos obtenidos a través de Internet a un ordenador denominado "ftp.laredcafe.com" ubicado en el bar LRCC sito en la calle C. de P. de M., almacenandolos en el directorio denominado "jfs" correspondiente al usuario "Hispahack", sin que conste acreditado que el acusado JFS, mayor de edad y sin antecedentes penales, participase en esa entrada ilegal, obtención y transferencia de datos informáticos.

FUNDAMENTOS DE DERECHO

PRIMERO.- Al abordar con mayor detenimiento las cuestiones previas planteadas por la defensa del acusado al comienzo del juicio oral, enseguida se advierte la escasa consistencia de las alegaciones en que se funda la declaración de nulidad pretendida, pues si por una parte, y con referencia a las investigaciones realizadas por los miembros de la Guardia Civil adscritos a la Unidad Central Operativa, éstas no precisaban de denuncia previa por parte de los afectados, ya que, aunque asi sea con relación a determinadas figuras delictivas que pueden cometerse por medios informáticos o telemáticos, como es el caso del descubrimiento y revelación de secretos que tipifica el art 197 del vigente Código Penal, y conforme establece el art 20l.l del mismo Código, no ocurre lo mismo, sin embargo, con relación a otros delitos como es precisamente, aquél en que se centra la acusación formulada en esta causa, tipificado en el art. 264.2 del citado cuerpo legal, cuya persecución y castigo no se condiciona a la previa denuncia, siendo ésta en todo caso un requisito de procedibilidad una vez determinada la conducta punible y su calificación juridico penal, pero no un óbice para la actuación de investigación de conductas supuestamente delictivas, al margen de su concreta calificación, que corresponde a las fuerzas y cuerpos de seguridad del Estado, por otra parte, y en lo que atañe a la pretendida vulneración del derecho fundamental a la intimidad y al secreto de las comunicaciones que corresponde al acusado. debe señalarse que las investigaciones realizadas respecto del mismo no han incidido en ninguno de esos derechos, y su identificación fue posible, según explica el atestado, después de haber recibido un mensaje de correo electrónico alertando sobre las actividades de unos supuestos "hackers" informáticos, al que se adjuntaban fotografías de varios de los integrantes de ese grupo, uno de ellos identificado con las iniciales Jfs, accediendo posteriormente a una página de información pública ubicada en un proveedor de Internet de Estados Unidos que, según la información contenida en la misma, pretendía ser la página de un grupo llamado "Hispahack", y en la que aparecia un artículo atribuido a jfs, y tras realizar diversas gestiones lograron localizar en lnternet un ordenador conectado de nombre "jfs.hispahck.org" ubicado en la empresa GL de Gibraltar que, por medio de AAO, lograron averiguar que había sido dado de alta en la red por el acusado. Bien es cierto que para la identificación de otros supuestos integrantes de aquel grupo se acudió al proveedor en España de lnternet a fin de conocer su identidad mediante su dirección de correo electrónico, pero además de no ser éste el caso del aquí acusado, tampoco cabe entender que ello constituyese vulneración alguna del derecho fundamental al secreto de las comunicaciones, ya que no se tuvo acceso al contenido de ningún mensaje transmitido mediante correo electrónico y sí sólo al nombre de la persona que utilizaba la dirección correspondiente, de la misma manera que podría haberse identificado a un abonado del servicio telefónico a través de su número de abonado, no suponiendo ello violación de derecho fundamental alguno, ni siquiera de las prescripciones que para el acceso y transmisión de datos personales contiene la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal, pues la propia Ley excluye de la necesidad del consentimiento del afectado la recopilación de datos que requiera el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (art. 6.2), especialmente cuando la información al afectado impida o dificulte la persecución de infracciones penales o administrativas (art. 22.1), quedando en todo caso limitada la recogida y tratamiento automatizado de datos de carácter personal por las fuerzas y cuerpos de seguridad del Estado, sin el consentimiento de las personas afectadas, a aquellos supuestos y categorías de datos que resulten necesarios para la represión de infracciones penales (art. 20.2). En suma, no cabe sino reiterar aquí nuevamente el rechazo a la pretensión de nulidad de parte de las actuaciones llevadas a cabo en esta causa que plantea la defensa del acusado. Por lo demás, y en contra de lo que sostiene dicha parte, no se cuestiona aquí el ejercicio de la libertad de expresión través de lnternet, sino que el enjuiciamiento se centra en una actividad que con la expresión anglosajona "hacking" (intrusismo informático) hace referencia a un conjunto de comportamientos de acceso o interferencia no autorizados a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización o más allá de lo autorizado, conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables, y aún merecedoras de sanción penal si -como suele ser lo habitual- atentan contra sistemas o equipos informáticos particularmente relevantes que, por razón del contenido de la información que procesan o almacenan y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales, afectan gravemente a un interés supraindividual o colectivo, de manera que plantear en esta sede una adecuada tutela penal autónoma frente al intrusismo informático no puede en modo alguno considerarse un exceso de reacción penal.

SEGUNDO.- Los hechos que se declaran probados en esta resolución son el resultado de una apreciación en conciencia de las pruebas practicadas en el juicio, conforme a lo dispuesto por el art. 741 de la Ley de Enjuiciamiento Criminal, y así, en efecto, el informe elaborado en su momento, y ratificado en dicho acto plenario como testigo, por JBT refiere la existencia de un ataque a los sistemas informáticos de la UPC con resultado de obtención de privilegios de administrador e instalación de programas "sniffers", afectando al menos a dieciséis máquinas servidoras y haciendo uso de herramientas para capturar información en las menos cinco de ellas, concretamente identificadores y claves de acceso de otros usuarios, ataque realizado

desde una máquina perteneciente a la UO y que remitió la información obtenida a otra máquina instalada en PM (folios 15 y 16). No cabe reputar acreditada, sin embargo, la autoría que de tales hechos se atribuye al acusado JFS, pues si bien existen fundadas sospechas de que pudo tener algún tipo de participación en ellos, ya que por una parte él mismo reconoce su pertenencia al grupo denominado "Hispahack" y la utilización del apodo "jfs" , que corresponden al usuario y directorio, respectivamente, del ordenador instalado en el Bar "LRCC" al que se transfirieron los datos obtenidos en el sistema informático de la UPC, habiéndose comprobado además, en el exámen del disco duro de los ordenadores que tenía en su domicilio de Martorell, intervenidos en la diligencia de entrada y registro practicada en el mismo, según expresa el perito JIG, la presencia de programas para aprovechar las vulnerabilidades de otros sistemas, ficheros de claves cifradas de usuarios de servidores y resultados de 'sniffers" que incluyen identificadores de usuarios y llaves de acceso a máquinas de la UB y a la UO, sin embargo tales sospechas no alcanzan la categoría de indicios bastantes como para desvirtuar totalmente la presunción de inocencia en cuanto a la concreta participación que en esos hechos se le atribuye, pues si por una parte el acceso al ordenador de PM, y a través de él al directorio "jfs", se hallaba al alcance de cualquiera que lo hiciese a través de usuario "Hispahack", en el que el mismo perito, al examinar el disco de dicho ordenador también intervenido tras la diligencia de entrada y registro practicada en el local donde se hallaba instalado, ha comprobado la existencia de ficheros de datos y utilidades relacionadas con los problemas de seguridad de los sistemas Unix, conteniendo información sobre vulnerabilidades de máquinas, programas para explotar fallos de seguridad, "sniffers" y otras utilidades conocidas como "utilidades de hacking", al alcance de cualquiera que pudiera acceder a dicho ordenador como usuario "Hispahack", ni el informe de FOF sobre el ordenador de la Universidad de Oviedo, a través del cual se accedió a los sistemas de la UPC, ha podido definir el origen de la intrusión no permitida a través de Internet, constatando la existencia de un directorio compartido accesible a cualquier máquina, sin claves, montado por otras dos máquinas desconocidas, ni el examen de los ficheros contenidos en los discos instalados en los ordenadores del acusado ha permitido establecer que éste poseyese información de aquellos sistemas. Ya el propio testigo JBT admite que posiblemente la persona que usaba los "sniffers" era la misma persona que los instaló, pero no puede afimarlo con certeza, el perito JIG afirma que los ficheros con códigos de usuarios y llaves de paso detectados en las máquinas del acusado fueron generados por "sniffers" que alguien (sin precisar quién) instaló en servidores de diferentes organizaciones, y conviene con el también perito PFG en que entre tales ficheros no se hallaba ninguno de password de la UPC. No apareciendo acreditado, por tanto, más allá de toda duda razonable, que fuese el acusado quien alteró los programas contenidos en el sistema informático de dicha Universidad haciendo necesaria su total reinstalación, que es la conducta sancionada penalmente que se le atribuye, no cabe llegar a otro pronunciamiento que el de su libre absolución.

TERCERO.- Procede declarar de oficio las costas ocasionadas de conformidad con lo establecido por los arts. 239 y 240.1º de la Ley de Enjuiciamiento Criminal

Vistos los preceptos legales citados y demás de general y pertinente aplicación,

F A L L O

Que debo de absolver y absuelvo libremente a JFS del delito de daños de que venía siendo acusado en este procedimiento, declarando de oficio las costas ocasionadas.

Líbrese y únase certificación de esta resolución a las actuaciones, con inclusión de la original en el Libro de Sentencias.

Así por esta mi sentencia, definitivamente juzgando, lo pronuncio mando y firmo.
CASO !HISPAHACK: INFORME FINAL DE LA DEFENSA

1.- ABSOLUCION

Los hechos enjuiciados no son delito, y tampoco existen pruebas que permitan atribuirlos a mi cliente.

2.- INEXISTENCIA DE DELITO

Nadie ha podido examinar, exceptuando a los denunciantes y sus subordinados, qué ocurrió exactamente en el ordenador de la UPC la noche de la Diada de 1997. La única información existente sobre qué ocurrió aquel día, es un texto impreso, proveniente, según los denunciantes, de un log generado por un sniffer en el ordenador de la UPC, al que ningún perito, ni siquiera el judicial, ha tenido acceso. Y estas dos palabras tan extrañas para el hombre corriente e incluso para los juristas, log y sniffer, hacen referencia a un archivo de texto que ha podido ser generado por cualquiera con un ordenador cualquiera. Esa es la gran prueba de la acusación.

Pese a las dudas que debe generar una prueba de origen tan espúreo como esta, vamos a hacer entre todos un ejercicio de credulidad. Vamos a olvidarnos de lo que dice la Constitución y la Ley de Enjuiciamiento

Criminal sobre esas cosas tan bonitas de la presunción de inocencia, y que la carga de la prueba en el proceso penal corresponde a la acusación. Vamos, por un breve instante, a dar un voto de confianza a la prueba, y vamos a hacer un experimento. Veamos que puede sacarse de esta prueba.

Del fichero impreso no se puede extraer información acerca de quién entró, ni cómo lo hizo. Tampoco se sabe que contienen los ficheros del ordenador. En el texto impreso sólo salen los nombres, pero no se ha hecho una pericial para decirnos qué contenían los ficheros. Lo que sí está claro es que no borra ninguno, ni introduce datos adicionales, ni virus. Tampoco se sustrae información confidencial alguna. No se ha encontrado en ningún ordenador la lista de passwords de la UPC. En consecuencia, ¿donde está el delito? ¿En que hayan tenido que mejorar la seguridad? Siguiendo la línea expositiva del Ministerio Fiscal, que ha realizado una comparación con el hecho de que si se ha abierto una puerta, aunque sea sin forzarla, hay que cambiar la cerradura, debemos afirmar rotundamente, que en este caso no había puerta. Y puestos a buscar comparaciones, sería como si el propietario de una nave industrial, en la que nunca ha habido puerta, reclama contra unos okupas para que le pongan una puerta blindada, o que un latifundista pida a los que han ocupado sus tierras, hasta entonces sin vallas, que le financien las alambradas de espino. El presunto hacker, si alguna vez entró, no lo hizo por la puerta principal. No falseó contraseña alguna. Simplemente entró por cualquiera de los muchísimos fallos de seguridad de la UPC. Suerte tuvo el administrador que hoy ha declarado, de que no hubiese ninguna intención maligna. Y debe estar agradecido, si no hubiese sido por el susto, no se hubiese reforzado nunca la seguridad. No hay menor vacuna para la seguridad de un sistema que el hacking blanco.

Debo hacer ahora una mención al carácter fragmentario del Derecho Penal, cuya aplicación debe reservarse a los ataques más graves a los bienes jurídicos protegidos.

Los tipos delictivos de revelación de secretos, de daños, e incluso los que protegen la seguridad atómica o la defensa nacional, susceptibles de ser atacadas mediante hacking, están claramente delimitados en nuestro código. El simple acceso a un sistema para verificar su seguridad, incluso dándose un paseo por el mismo, no puede ser delictivo si no hay sustracción de secretos o daños intencionados. Los tipos penales existentes no permiten incriminar la simple intrusión en un sistema: deben interpretarse restrictivamente, y en beneficio del reo. Si se quiere establecer un castigo para dicha conducta, debería redactarse un nuevo tipo penal.

En una reciente sentencia del Tribunal Supremo Noruego, se determinó que el acceso a un sistema por sí mismo, no constituye delito. En España no existe jurisprudencia que pueda citar. Por eso este juicio es un momento histórico: lo que Su Señoría determine hoy, se va a convertir en la primera teoría jurídica sobre el hacking en España. Las leyes nunca son neutras, pero es la interpretación la que debe adecuarlas a la realidad social. Y sólo los ataques más graves a los bienes jurídicos protegidos deben tener una respuesta penal.

La mejor prueba de la defensa nos la ha proporcionado la Guardia Civil en los folios 402 y 403 del sumario, al dirigir una curiosa recomendación al Juzgado de Instrucción para que se le pasase el caso al E. En dicha recomendación, se indicaba incluso qué debía buscarse en los ordenadores a peritar: En la página 402 se indica textualmente que se debe verificar si en dichas máquinas:

a) Hay información relacionada con los ataques a la UPC.

b) Se encuentra el programa o utilidad necesarios para su realización.

c) Aparecen ficheros conteniendo información obtenida en dichos ataques.d) Existe logs que demuestren la existencia de los mencionados ataques.

e) Cualquier otra información que sea de interés para la investigación.

Nada de lo que buscaba con tanto ahínco la Guardia Civil se ha encontrado. No puede pues, pretenderse que existen pruebas del delito por el que se acusa.

3.- NULIDAD DE LA PRUEBA

Hemos dicho antes que hacíamos un ejercicio de credulidad, y dábamos provisionalmente por buenas las pruebas aportadas por la acusación. Pasemos ahora página, y examinemos si dichas pruebas se obtuvieron lícitamente. Porque no sólo no prueban nada, sino que además son nulas, y de acuerdo con el artículo 11.1 de la Ley Orgánica del Poder Judicial, no surtirán efecto las pruebas obtenidas vulnerando derechos fundamentales. En base a la doctrina del fruto del árbol envenenado, ampliamente desarrollada en la jurisprudencia del TS y el TC, todas las pruebas derivadas de una prueba nula, son también nulas.

Las pruebas aportadas no pueden tener ningún valor probatorio, y ello porque no se respetó por las fuerzas policiales, ni por los denunciantes, el derecho fundamental a la intimidad y al secreto en las comunicaciones. Ningún reproche se ha de hacer a la Juez de Instrucción, cuyo trabajo fue impecable. Pero nos hallamos ante

un caso, en el que desde su mismo inicio, debía haber tenido intervención judicial. Resulta absolutamente increíble que unos hechos que presuntamente ocurren el día 11 de septiembre, se investiguen sin denuncia alguna, practicándose hasta peticiones de passwords a proveedores de Internet, dejando para el final, concretamente el día 25 de marzo de 1998, la confección y tramitación de la denuncia.

A Internet, exceptuando algunas instituciones de gran poder económico, no se puede acceder sino es por teléfono. Y cualquier intervención telefónica requiere autorización judicial. Lo que se tenía que haber hecho en el presente caso, y en cualquier otro similar, al detectar un presunto intruso, es avisar inmediatamente al Juzgado de Guardia. Porque sólo la fe pública judicial puede legitimar un archivo de texto como el que se nos ha pretendido presentar como prueba. Porque sólo un Juez de Instrucción puede autorizar que se examine una comunicación telefónica, como es Internet. Porque sólo el Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, pueden solicitar datos de usuarios registrados en bases de datos, de conformidad con el artículo 11 d) de la Ley Orgánica de Tratamiento Automatizado de los Datos de Carácter Personal, ley que desarrolla lo dispuesto en el artículo 18.4 de la Constitución.
Toda la investigación de este caso se hizo sin contar con el Juez, exceptuando las órdenes de entrada y registro en domicilios particulares.
Resulta que la Guardia Civil, más de un mes antes de tener la denuncia, había pedido a RTB, proveedor de Internet, todos los datos de un tal J.R., del que todos podemos saber hoy que usaba como contraseña de acceso el nombre de una especialidad médica, según puede verse en el folio 113 del sumario. No hay pruebas de que dicha contraseña se usase, pero lo cierto es que La Guardia Civil pudo tener acceso durante demasiado tiempo antes de las detenciones, a toda la correspondencia electrónica del señor J.R.: toda la correspondencia que quizás cruzó con los restantes acusados. De la misma forma, se pidieron datos confidenciales de usuarios de I, S, y algún otro proveedor.

Todas estas pruebas debía haberlas solicitado, y autorizado, el Juez, al que se le privó de ejercer su autoridad, única legitimada para controlar que en la investigación no se vulneran derechos fundamentales.

Durante la posterior instrucción del sumario, como ya he dicho, la actuación jurisdiccional fue impecable. Sin embargo, se produjo un hecho fuera de la sede judicial, y por consiguiente del control de la Juez de Instrucción, en la prueba pericial que pueden producir la nulidad absoluta de la misma.

El perito tuvo acceso al correo electrónico personal del acusado. Dichos mensajes no dicen nada importante para la causa, pero lo cierto es que el perito accedió a los mismos, y ése es el problema que invalida toda la prueba pericial. Porque la correspondencia, sea postal, telegráfica, o electrónica, debe examinarse de conformidad con lo dispuesto en el título VIII del libro II de la Ley de Enjuiciamiento Criminal. En especial, el artículo 586, que especifica claramente que la operación se practicará abriendo el Juez por sí mismo la correspondencia, y después de leerla para sí, apartará la que haga referencia a los hechos de la causa y cuya conservación considere necesaria.El precepto no es caprichoso, está pensado así para asegurar la protección del derecho fundamental a la intimidad. Derecho vulnerado por el perito, al no abstenerse y pedir que fuese el Juez, en todo caso con su auxilio, el que examinase la correspondencia: ninguna diferencia ha de haber entre la postal y la electrónica.

4.- LAS PRUEBAS DE CARGO QUE NO SON NULAS, SON POCO FIABLES

La prueba, para ser admisible, debe tener unas características de fiabilidad de las que adolece el informe de los técnicos del E. Y ello no es porque no se trate de técnicos de gran prestigio, todo lo contrario. Precisamente por ello se debían haber abstenido de realizar dictamen alguno, en un asunto en el que estaba implicada la misma Universidad que da cobijo al E. Nos hallamos en un caso en que lo que estaba en juego era precisamente el prestigio de la Universidad, del administrador de su sistema informático, y del E. Eran motivos más que suficientes para abstenerse. Expertos en seguridad en redes telemáticas los hay por todas las Universidades españolas, como hemos podido comprobar. ¿Por qué se intentó hacer creer al Juzgado de Instrucción que sólo había expertos en el E.? ¿O es que el E y la UPC no querían que ningún otro técnico, que ninguna otra Universidad, supiese cuales eran los fallos de su sistema? Prefiero creer que no es esta la causa. Pero desde luego invalida la prueba.

5.- NO HAY EVIDENCIA DE QUIEN PUEDE SER EL AUTOR

Con independencia de lo ya manifestado acerca de la inexistencia de delito, debe quedar claro que no hay evidencia alguna que los hechos denunciados fuesen realizados por mi defendido.

La razón por la que fue detenido no es otra que su nick: JFS, y su pretendida pertenencia a un grupo de estudiantes de seguridad, !Hispahack. El famoso log de la noche de la Diada, cuya legitimidad ya hemos puesto en duda, indica que hubo una conexión con un ordenador de PM, usando la palabra clave Hispahack y accediendo al directorio JFS.

Sin necesidad de acudir a la prueba pericial presentada por la defensa, del propio informe del E, se desprende que el directorio JFS era accesible por infinidad de personas, con privilegios de lectura y escritura. Y una de ellas, curiosamente, era la que había dado de alta la cuenta, tenía administración local y remota del sistema, y ha depuesto hoy como testigo. No es mi labor acusar, sino defender, pero debe decirse que tan culpable podría ser esta persona como mi representado, y tan pocas pruebas hay contra uno como contra otro.

En nuestro derecho penal, la responsabilidad debe individualizarse. La pertenencia a un grupo no es en sí misma constitutiva de delito alguno. Tampoco se ha acreditado que Hispahack sea la peligrosa banda criminal que la Guardia Civil publicitó a los informadores, al hablar de su brillante desarticulación. Si se busca la palabra JFS, en Internet, se encontrarán miles de referencias. Pero no basta con tener la desgracia de que el nombre de un nick, de solo tres letras, coincida con un directorio estigmatizado. Hay que demostrar que fue JFS quien accedió a la UPC, si accedió alguien.

El tantas veces citado log de la noche de la Diada no revela la IP de origen, esto es, desde donde accedía el presunto hacker. Se sabe que hacía cosas entre O, B y PM, cosas no dañinas, por otra parte. Pero no se sabe de donde venía.

Si estuviésemos en un caso de delito grave, un asesinato, se debería demostrar que la noche del crimen el acusado estaba en un determinado sitio, haciendo una determinada cosa. Nadie ha testificado que viese a JFS acceder a Internet, y a través de Internet, a la UPC. Ni se sabe la IP origen del presunto atacante, ni se ha demostrado que el acusado estuviese sentado delante del ordenador, conectado al teléfono. No somos nosotros quienes hemos de buscar coartadas, es la acusación quien tiene que probar aquello que afirma.

No hay pruebas ni en la UPC, ni en O, ni en PM, ni en los ordenadores de mi cliente, del acceso a la UPC. Se le ha relacionado con los hechos sólo por su nick. Ninguno de los datos encontrados en los ordenadores de mi cliente, revelan práctica delictiva alguna. Simplemente, como nos han dicho los peritos, evidencian que hacía prácticas de seguridad, mediante los mecanismos habituales de aprendizaje. No revelan entradas en ningún sistema, y desde luego no aparece dato alguno de la UPC.

La posesión de cracks sólo es delictiva en tanto sirvan para desproteger programas de ordenador. No son lo mismo que los cracks de contraseñas, que sirven para poder acceder a las mismas en caso de urgencia. Algo que todo buen administrador debe saber hacer, del mismo modo que las fuerzas policiales.

6.- NO SE HAN ACREDITADO LOS DAÑOS, NI SU IMPORTE.

La cantidad que se reclama por daños no tiene justificación alguna. Aparte de lo que ya se ha dicho de que no se puede cargar sobre las espaldas de nadie la responsabilidad de garantizar la seguridad de un sistema, incluso en el supuesto que se hubiese podido acreditar la intrusión, no hubiese sido necesario paralizar nada para prevenir fallos futuros de seguridad. Bastaba blindar adecuadamente el sistema, como se debía haber hecho desde un inicio, y cambiar las contraseñas, como de hecho se hace periódicamente. No tiene ninguna justificación lo reclamado, pero además tampoco se han probado los gastos.

7.- DESCRIMINALICEMOS LA RED

Quiero acabar mi intervención hablando de derechos humanos. Internet es la culminación histórica de un proceso global de desarrollo del pensamiento humano. Nunca como ahora ha sido posible la comunicación de las ideas: Internet es el tejido neuronal de la conciencia colectiva de la humanidad. No obstaculicemos la libertad de pensamiento, la libertad de expresión. Delitos los ha habido siempre, estaban todos inventados antes de que existiese la Red. Pero lo que hoy se ha pretendido juzgar aquí es un presunto delito completamente virtual, en todos los sentidos, que no ha tenido repercusión alguna fuera de la misma Red. No nos engañemos: las causas por las que se inició la investigación no son otras que la incomodidad que representaba para determinados poderes, públicos y privados, la existencia de una publicación electrónica tan libertaria como Mentes Inquietas. Muy posiblemente nunca hubiese existido el caso Hispahack si desde Mentes Inquietas no se hubiesen denunciado determinados abusos de empresas monopolísticas, y la colusión de intereses de las mismas con fuerzas de seguridad.

Ya he indicado anteriormente que estamos en un momento histórico: hoy se va a sentar jurisprudencia en España sobre qué debe ser admitido, y que no, en la Red. Una red donde el intercambio de ideas conduzca al progreso de la Humanidad. Donde el conocimiento no sea, como en algunos momentos negros de nuestra historia, un crimen: afortunadamente las páginas binarias no pueden enviarse a la hoguera. Confiamos en Vd., Señoría. Muchas gracias.

PFG, Ingeniero de Telecomunicaciones, Doctor en Informática, Profesor Titular de Escuela Universitaria, y desarrollando mi trabajo de investigación sobre temas de seguridad, emito el siguiente dictamen a petición de la defensa.

I.- Consideraciones previas

1.- La seguridad del sistema operativo UNIX

1.1 Un sistema operativo puede estar pensado para el uso individual o para el uso de un colectivo de personas.

1.2 El sistema operativo UNIX, por su naturaleza, es un sistema operativo multi-usuario. Esto significa que múltiples usuarios pueden compartir recursos de un ordenador: ficheros, aplicaciones, etc.

1.3 De todas maneras, debe poder discriminarse qué usuarios tienen derecho a acceder al sistema y sobre qué recursos del mismo.

1.4 La manera de realizarlo es a través de la interrogación al usuario de un identificador personal (login) y una palabra de paso (password)

1.5 Cualquier acceso a la máquina, tanto si es de forma local (en frente del propio ordenador) como si es de forma remota (utilizando las redes de comunicaciones), implica que el usuario se ha de identificar previamente a través de su login y password.

1.6 El sistema contiene un fichero que le permite verificar, en base al login y password, si el usuario que intenta acceder al sistema está autorizado o no: es el conocido como fichero de passwords.

1.7 El nombre de fichero de passwords conduce a la confusión, dado que puede parecer que contiene los passwords de los usuarios del sistema; en realidad no es así.

1.8 El fichero de passwords sólo contiene una información cifrada en relación al login y el password.

1.9 Cuando el usuario introduce su login y password lo que hace el sistema operativo es repetir la operación de cifrado con estos datos y confrontar si el resultado de este cifrado coincide con el contenido en el fichero de passwords.

1.10 Por tanto, de los puntos 1.7-1.8-1.9, se deriva que de un fichero de passwords no pueden extraerse passwords de los usuarios, porque de hecho no están.

1.11 Es más, ni tan siquiera el administrador del sistema (que realiza operaciones de altas de usuarios, bajas de usuarios, concede derechos de accesos a recursos, etc.) puede, ni debe, llegar a conocer el password personal de ningún usuario particular.

1.12 Por su naturaleza, el fichero de passwords debe ser accesible a todos los usuarios del sistema, pues este acceso es paso previo necesario para acceder al mismo.

1.13 Esta característica, 1-12, probablemente no deseada, es plenamente conocida por todos los administradores de sistemas UNIX.

1.14 De los puntos anteriores, 1.12-1.13, se deriva que la seguridad del sistema no debe residir en la confidencialidad del fichero de passwords.

1.15 A pesar de lo dicho en los puntos 1.10-1.11, existe un posible ataque por fuerza bruta: probar para un login determinado los posibles passwords que pudiera haber escogido el usuario asociado a ese login.

1.16 Por lo dicho en 1.14-1.15, la seguridad del sistema reside en que los usuarios escojan passwords robustos, es decir, que no sean fáciles de "adivinar".

1.17 Es tarea del administrador del sistema informar y asesorar a sus usuarios sobre el tipo de password que ha de ser escogido, y también vigilar, realizando él mismo ataques por fuerza bruta, para controlar que sus usuarios, a pesar de sus recomendaciones, no hayan escogido passwords débiles.

1.18 Asimismo, es tarea del administrador hacer que de forma automatizada, el sistema obligue a los usuarios a cambiar de password periódicamente.

1.19 Una vez introducido el login y password correcto, el sistema de forma automatizada, y en base a la configuración introducida por el administrador del sistema, permite al usuario acceder a los recursos a los que tiene derechos (aplicaciones comunes, sus ficheros personales, etc.)

1.20 Inicialmente el sistema basado en login y password, permite al administrador imputar acciones particulares a usuarios particulares.

1.21 Cada usuario dispone de un login, que puede ser públicamente conocido, y de un password que sólo debe ser conocido por él (véase 1.10 y 1.11).

1.22 Un sistema bien configurado registra las operaciones relevantes que realizan los usuarios en un fichero que recibe el nombre de fichero de log.

1.23 Estos ficheros de log son de utilidad para el administrador para rastrear funcionamientos incorrectos del sistema, y acciones incorrectas realizadas por parte de los usuarios, permitiéndole corregir estas situaciones.

1.24 Los ficheros de log son ficheros de texto ordinarios, y que por tanto pueden ser manipulados por parte del administrador sin ningún problema.

1.25 De 1.24 se deriva que, a priori, no debiera considerarse la información contenida en un fichero de este tipo, como información de veracidad incuestionable.

1.26 A pesar de lo dicho en 1.20-1.21-1.22, si múltiples usuarios comparten un login y password, no hay manera de discriminar cuál de ellos ha realizado las operaciones que puedan quedar registradas en el fichero de log.

2.- Las conexiones en Internet

2.1 Para poder intercambiar información entre ordenadores a través de la red Internet, cada ordenador debe estar identificado con lo que se conoce como una dirección de red.

2.2 La dirección de red que utiliza cada ordenador debe ser única, dado que en caso contrario, el sistema no funcionaría correctamente.

2.3 Para no obligar a los usuarios a recordar la dirección de red del ordenador con el que desean dialogar remotamente, existe una segunda manera que permite referenciar los ordenadores que se denomina nombre de dominio (o nombre simbólico).

2.4 Existe una aplicación telemática que se encarga de realizar la traducción de un nombre de dominio a su correspondiente dirección de red.

2.5 A priori, puede parecer que la dirección de red identifica biunívocamente el ordenador, y por ende podría ser que también al usuario, que ha realizado una conexión remota.

2.6 Desafortunadamente, estas direcciones de red son manipulables por parte de los usuarios, de tal forma que un usuario puede configurar su ordenador con una dirección de red que realmente no le corresponde.

3.- La realización de peritajes telemáticos

3.1. Para realizar cualquier peritaje es fundamental disponer de información, e información fiable, sobre los hechos acaecidos.

3.2 Por desgracia, en el caso de sucesos telemáticos, la información de la que se puede disponer en la mayoría de los casos es escasa, o por su naturaleza es fácilmente manipulable (véanse 1.24 y 2.6).

3.3 Sorprende que se encargue el peritaje de la información contenida en el material incautado a una de las partes afectadas en el procedimiento (la parte denunciante): el E de la UPC.

3.4 No se duda de la competencia del personal que lo integra, ni tan siquiera que en este caso hayan actuado maliciosamente, pero repetimos que sorprende que sean denunciantes y peritos en el procedimiento seguido.

3.5 Destacamos de todas formas lo recogido en el folio 14 del procedimiento, manifestado por el propio E: "No es por tanto responsabilidad de E la de localizar a los atacantes, sino la de conocer sus métodos".

3.6 De todas formas, queremos reiterar y recalcar que no se pone en duda que toda la información que contiene el procedimiento no ha sido manipulada por los peritos y técnicos que han intervenido en la elaboración de los correspondientes informes.

3.7 No es así en el caso de la información concreta que contienen los ficheros analizados que podría haber sido manipulada por parte de los hackers que hubieran accedido a los sistemas.

4.- El hacking "blanco"

4.1 Definimos el hacking blanco como aquellas acciones realizadas por usuarios no autorizados, pero sin perseguir fines destructivos.

4.2 Encajan en la definición anterior, 4.1, los hackers que acceden sin autorización a sistemas remotos con el objetivo de conseguir tiempo de ejecución del ordenador, ficheros de passwords, etc, pero que no realizan, ni intencionada ni accidentalmente, la manipulación de información que no les pertenece. Es decir, no borran información de usuarios autorizados, no revelan información que debe permanecer confidencial, etc.

4.3 En ocasiones será difícil discriminar donde empiezan y donde acaban las acciones inocuas y las nocivas; la frontera no será siempre clara.

4.4 Parece exagerado "criminalizar" a un grupo de jóvenes que sólo persiguen aprender; el deseo de aprender, para alguien que procede del mundo universitario, siempre es loable.

4.5 De hecho no sólo aprenden los hackers, sino que indirectamente los administradores de sistemas también salen beneficiados.

4.6 Los "agujeros" de seguridad que detectan los hackers sirven para que los administradores mejoren la seguridad global de sus sistemas.

4.7 El punto 4.6 puede no parecer relevante, pero si pensamos que estos agujeros pueden ser utilizados para realizar acciones realmente maliciosas, que alguien las ponga de manifiesto es de gran utilidad.

4.8 También es cierto que sería preferible que los hackers informaran directamente a los administradores, y que estos no tuvieran que enterarse una vez producido el ataque y por otras vías.

4.9 No obstante, el E de la UPC, puede dar buena cuenta de que mucha de la información que manejan, y que les permite dar asistencia en relación a la seguridad de sistemas telemáticos, la han obtenido después de que un hacker realizara acciones no autorizadas en otros sistemas telemáticos.

II.- Sobre los hechos y daños descritos en los informes técnicos y periciales

5.- Hechos y daños en general

5.1 Las mayoría de los hechos descritos en los informes periciales y técnicos que se encuentran en el procedimiento no se refieren a la UPC y ni tan siquiera parecen relevantes para el procedimiento seguido en esta causa.

5.2 Siendo la acusación la de un delito de daños contra los intereses de la UPC, parece que deberíamos centrarnos en la información relacionada con ésta.

5.3 A pesar del punto 5.2, empezaremos recogiendo algunas de las informaciones extraídas del procedimiento.

5.4 Según consta en los folios 5 y 7 del procedimiento, la Guardia Civil manifiesta que un grupo de hackers han realizado las siguientes acciones:

5.4.1 Acceso no autorizado al ordenador del Congreso de los Diputados de Madrid.

5.4.2 Acceso no autorizado a los ordenadores de un proveedor de servicios de Internet de Girona, además de sustracción y difusión de datos personales y palabras de paso de 2500 usuarios del mismo (ver también folios 301 y 302).

5.4.3 Acceso no autorizado y daños en los sistemas informáticos de la UO (ver también folio 532, en el que además se añade que también acceden a ordenadores de la UB).

5.4.4 Intento de acceso no autorizado a ordenadores de la NASA.

5.5 En los ordenadores del Sr. JFS se han encontrado (ver folio 531) ficheros de passwords, utilidades de "pirateo informático", ficheros que contienen datos (ficheros de passwords) de la UO y de la UB, procedentes de sniffers. No se indica ninguna información relacionada con la UPC.

5.6 Según el peritaje realizado por el E (ver folio 531) el Sr. JFS ha descifrado claves de usuario (aproximadamente 414); vista la explicación realizada en 1.7 a 1.11, se entiende que la anterior afirmación es una licencia expresiva del autor del peritaje.

6.- Hechos y daños relativos a la UPC

6.1 El sistema informático de la UPC sufrió una entrada ilegal por usuarios no autorizados en 16 ordenadores servidores de la UPC, provocando una serie de daños en los mismos (ver folio 3)

6.2 La entrada ilegal (sic) se produce el 11 de septiembre de 1997 a las 4:16 horas a través de Internet, desde un ordenador ubicado en la UO denominado proy6.etsiig.uniovi.es.

6.3 Una vez realizada la entrada los atacantes:

6.3.1 Obtienen privilegios de los responsables técnicos de los 16 ordenadores servidores afectados de la UPC.

6.3.2 Suplantan su personalidad.

6.3.3 Capturan datos personales de usuarios como sus palabras de paso (passwords), a través de un programa informático denominado "sniffer" o "rastreador".

6.3.4 Se conectan a un ordenador, a través de Internet, denominado ftp.laredcafe.com ubicado en el Bar LRCC de PM.

6.3.5 Usan para ello el nombre de usuario (login) Hispahack y la palabra de paso (password) hhpax18.

6.3.6 La información obtenida en 6.3.3 se deposita en el directorio o apartado jfs del ordenador de 6.3.4

6.4 Según consta en la diligencia de exposición de hechos (folio 4):

6.4.1 El acceso ilegal ha afectado a todos los usuarios del sistema informático de la UPC.

6.4.2 Han debido realizarse numerosos ajustes de seguridad desde su conocimiento.

6.4.3 El impacto económico o daños ocasionados pueden estimarse cercano a los 2 millones de pesetas.

III.- Sobre la autoría de los hechos

7.1 Jafasa "miembro de un grupo de hackers" (sic) utiliza el alias jfs en un artículo publicado en Internet, e indica la dirección de correo jafasa@hotmail.com (ver folio 6).

7.2 El Sr. ECE declara (folio 190) :

7.2.1 Que accede al ordenador ftp.laredcafe.com de PM, con el nombre de usuario !HISPAHACK creyendo que su clave era lerele.

7.2.2 Que contaba con un directorio de uso personal de nombre Stk

7.2.3 Que la cuenta se la dio alguien de !hispahack.

7.2.4 Entre otros nombres de directorio recuerda el directorio Jfs

7.3 Se han realizado acciones no autorizadas (folios 242 y 243) en una máquina de O desde los ordenadores que tiene por direcciones de red 194.224.182.113 y 195.5.73.45, con su correspondientes nombres de dominio info63.jet.es y id-45.arrakis.es, respectivamente.

7.4 El Sr. JBC "cree" (ver folio 301) que en base a un diálogo por Internet, con alguien que utiliza como apodo Stk, miembros del grupo !HISPAHACK participaron en el ataque descrito en 5.4.2.

7.5 El Sr. ECE declara (folio 378) que Jfs accede al ordenador ftp.laredcafe.com de Palma de Mallorca, con el nombre de usuario (login) !HISPAHACK.

7.6 El Sr. JFS declara (ver folio 385) que utiliza el apodo JFS.

7.7 El Sr. BVV declara (ver folio 440) que a petición de un usuario que utiliza como apodo Cure da de alta un usuario en el ordenador ftp.laredcafe.com con nombre de usuario (login) HISPAHACK.

7.8 Según el peritaje elaborado por el E (ver folio 531) un usuario que utiliza como nombre de usuario (login) thelobo:

7.8.1 Accede a la máquina ftp.laredcafe.com desde la consola (es decir, de forma local, y no remotamente).

7.8.2 Conoce la existencia y el contenido de la cuenta hispahack.

7.8.3 Además (ver folio 536) accede a datos concretos: el fichero SUN01.TXT de la mencionada cuenta de usuario.

7.9 Del análisis de la cinta de datos incautada en el procedimiento (ver folio 532) se deriva que el hacker que ha intervenido en la acciones maliciosas utiliza el login rewt y distintos passwords.

IV.- Conclusiones

8.- Sobre los hechos y los daños

8.1 Los hechos relativos a la entrada en los servidores de la UPC encajan dentro de la definición de hacking blanco descrito en el apartado 4.

3.3.1.- Tipo objetivo

El artículo 264 del Código Penal establece una pena de prisión de uno a tres años y multa de doce a veinticuatro meses para el 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.

En este caso el tipo objetivo no es el descubrir un secreto, sino causar daños a una cosa, en este caso los datos informáticos. Hemos de acudir al concepto de daño, y el resultado ha de ser la destrucción o inutilización de la cosa. En este sentido hay tratadistas que consideran que el sabotaje informático mediante virus sólo puede penarse si el virus destruye los datos, pero no si el ordenador únicamente actúa más lentamente. Entiendo que aunque no se produzca la destrucción total, el patrimonio ajeno ha de ser objeto de protección, y en consecuencia una agresión que suponga un perjuicio ha de ser castigada.

Hemos de preguntarnos, y muy seriamente, si el hecho de entrar en un sistema, por sí mismo, ya genera un daño: el que sufre el administrador, al descubrir que su sistema es inseguro, con las consiguientes horas de paranoia invertidas en la búsqueda de la invulnerabilidad. La respuesta está en la misma pregunta: si el sistema era ya inseguro, esa inseguridad no la ha creado el hacker, y en consecuencia no cabe hablar de daño, pues el deterioro que debería sufrir la cosa dañada es preexistente a la acción del intruso. Sólo podemos hablar de daño cuando hay destrucción de datos, cuando se rompe una puerta que antes no estaba abierta, no cuando se

---

8.2 No se observa la destrucción de ningún tipo de información y por lo tanto no hay daños en este sentido.

8.3 La sustracción de ficheros de passwords no supone, o no debería suponer, ningún gran desastre (véanse 1.10 y 1.14). Pero además:

8.3.1 Los passwords deben ser cambiados periódicamente (ver punto 1.18).

8.3.2 Notificar de forma masiva a los usuarios que deben cambiar de password consiste, sencillamente, en enviar un correo electrónico a un grupo de usuarios.

8.4 La reinstalación del sistema operativo parece que queda demostrado que era una necesidad para eliminar fugas de seguridad que presentaba el sistema (ver 4.6).

8.5 De lo descrito en 5.5 lo único que se puede concluir es que el Sr. JFS es un entusiasta del mundo de la seguridad telemática (ver a propósito 4.4).

9.- Sobre la autoría de los hechos

9.1 Eran múltiples los usuarios que podían acceder a la información contenida en la cuenta HISPAHACK del ordenador ftp.laredcafe.com (véanse 7.2, 7.5 y 7.8)

9.2 De 9.1 se deriva que cualquier usuario distinto del Sr. JFS pudo haber depositado la información en ese ordenador (según se describe en el punto 6.3)

9.3 De la información de ficheros de passwords encontrada en el ordenador del Sr. JFS sólo se deriva que la obtuvo del algún ordenador, que podría ser el que tiene por nombre ftp.laredcafe.com o no, pero no que fuera él quien la obtuviera de las fuentes originarias.

9.4 Todos los demás datos no apuntan a que el Sr. JFS haya realizado ninguna de las entradas en ordenadores ajenos descritas en los apartados 5.4 y 6.3.

Lo que hago constar, según mi leal saber y entender, en Barcelona, a veintiséis de mayo de mil novecientos noventa y nueve

franquea un paso expedito. La situación de inseguridad no ha sido creada por el hack blanco, sino por una administración negligente, que no ha protegido o encriptado adecuadamente el sistema.

Ello no obstante, en la mayor parte de las ocasiones, la responsabilidad no será tanto del administrador del sistema, como de los diseñadores de determinados sistemas operativos, que parecen más pensados para vulnerar la intimidad que para protegerla. Quizás le resulte mucho más rentable, al propietario de la máquina atacada, demandar civilmente a quien le puso a los pies de los caballos, que perseguir en vía penal a un hacker desconocido.

Lo primero que hace todo buen hacker es borrar sus huellas. Ello comporta el acceso al fichero de logs, para modificar cualquier referencia a su acceso. Si únicamente se borra aquella parte que hace referencia a las huellas, sin causar ninguna pérdida de datos adicionales, tampoco podrá hablarse de daños. Y si eso no se sabe hacer, que el aprendiz de hacker siga haciendo prácticas en su casa y en su red.

3.3.2.- Tipo subjetivo

Se trata de un delito que requiere ánimo de causar daño, si bien es posible la comisión por imprudencia, pero en tal caso los daños tendrían que ser superiores a 10 millones de pesetas para poder perseguirse penalmente. www.bufetalmeida.com

De acuerdo con la exposición anterior, y a modo de conclusión diremos que los daños al sistema informático no constituyen un subtipo agravado o cualificado de la figura de daños en cosa ajena como pretende el nuevo Código Penal. Estamos, por el contrario, ante una figura autónoma e independiente que posee unos caracteres propios y determinados, cuyo lugar más adecuado no es el capítulo de los daños, sino un capítulo independiente donde, al igual que en el Code penal francés, tuvieran cabida todas aquellas conductas que se dirigen hacia la utilidad del sistema informático en sí. De lege ferenda, sería conveniente, junto al cambio de ubicación de la figura, una descripción amplia de los comportamientos típicos con el fin de acoger las distintas formas de delincuencia informática, incluso las que surjan al compás de los avances tecnológicos; así como la previsión de una serie de agravaciones específicas como, a título de ejemplo, la comisión por parte de un empleado del sistema con especiales conocimientos técnicos o la causación de especiales perjuicios a empresas, Administraciones Públicas, etc[10].

4.- LA ESTAFA INFORMATICA

Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para acometer determinadas faenas. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, y, entre otras cosas, se han abierto nuevas perspectivas de

[10] Dra. Ana Cristina Andrés Domínguez. La Ley 1999-1.

consumo mediante el uso de Internet. Todos los que navegamos por Internet, conocemos que se venden cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es muy lógico, pues se ahorran muchos costes y amplían su potencial de mercado, por ejemplo, imagínese los costes que una empresa puede tener para establecer una sucursal en otra provincia de España, y ahora piense los costes que puede tener una empresa creando su propia página en Internet, con catálogos de sus productos o servicios, descripción de los mismos, precio, atención al cliente por correo electrónico, etc. (imagínese si lo que queremos es establecer una simple sucursal en otro país). Lógicamente todo depende del tipo de empresa de que se trate y del producto o servicio que venda, pero esta reflexión nos sirve para pensar en la importancia de la red para muchas empresas. Pero todo el monte no es orégano, y nos podemos encontrar con que la supuesta empresa nos manda productos que no son, no podemos reclamar directamente porque no sabemos dónde se ubica la empresa, o simplemente hemos hecho un pago con la tarjeta de crédito y no nos han dado el servicio o producto; todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio de una estafa, piénsese en dar número de tarjetas de crédito falsas pero que el robot acepta como válidas (conocido en el mundo de Internet como "carding"), etc. Con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos, por supuesto estos sólo son unos ejemplos relativos a la red, pero también se pueden dar otros casos.

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

Art. 248. 2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Este artículo es la mayor novedad del Código Penal de 1995, respecto de la estafa. Con este artículo se nos equipara con el resto de naciones de nuestro entorno cultural y social; pero además cubre la laguna legal que existía con anterioridad a este artículo, pues la informática, las telecomunicaciones, la tecnología, etc. avanza a pasos agigantados, y muchas veces el Derecho no reacciona a tiempo para regular las nuevas situaciones que se dan cada vez que hay un avance tecnológico.

Este artículo 248. 2 CP esta regulando una estafa normal y corriente, excepto que aquí no se engaña, ya que a una máquina no se la puede engañar, esto sólo se puede hacer a los humanos.

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

El ánimo de lucro ha de ser entendido como la intención de obtener un enriquecimiento patrimonial correlativo al perjuicio ocasionado. Este ánimo de lucro constituye un elemento subjetivo del tipo, y su ausencia hace que la conducta realizada sea atípica, y por tanto impune.

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

Por último, ha de existir un perjuicio para un tercero, que es la diferencia de valor entre lo que se atribuye a otro y lo que se recibe (si es que se recibe): si la contraprestación es de igual valor que la prestación otorgada, no hay delito, aunque pueda haber un perjuicio indemnizable por la vía civil; y si la contraprestación es de menor valor, puede haber un delito de estafa, aunque no haya civilmente perjuicio alguno.

El concepto "manipulación informática" es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Con todo lo anterior podemos definir la estafa informática como la "manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico a un tercero"[11]**.**

Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial.

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

Internet cuenta ya con un decálogo de prácticas ilegales. La Comisión Federal de Comercio (FCT) de Estados Unidos ha publicado una lista en la que figuran los 10 fraudes más comunes realizados al amparo de la Red. **Estafas en subastas, fraudes con tarjetas de crédito, falsas**

[11] Vives Antón - González Cussac.

oportunidades de negocio o engaños en vacaciones y viajes son algunas de las fórmulas que se recogen en la lista, elaborada a partir de las reclamaciones de los usuarios.

La Comisión Federal de Comercio (FTC) de Estados Unidos, el organismo que supervisa la competencia y se encarga de la protección de los consumidores, acaba de publicar una lista con los 10 fraudes más comunes que se pueden realizar a través de Internet. Así, el informe de la FTC es resultado de una iniciativa impulsada por los organismos de protección de los consumidores de varios países, entre ellos Alemania, Gran Bretaña o Canadá. 'Queremos que los artistas del fraude cibernéticos sepan que estamos montando una coalición de protección al consumidor en todo el mundo', manifestó Jodie Bernstein, responsable la Oficina de Protección a los Consumidores. El decálogo de la Comisión Federal de Comercio, realizado a partir de las denuncias efectuadas por los propios consumidores, considera que estos son los supuestos más frecuentes:

Las subastas: Algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.

Acceso a servicios de Internet: El consumidor recibe una oferta de servicios gratuitos. La aceptación lleva implícita el compromiso de contrato a largo plazo con altas penalizaciones en caso de cancelación.

Las tarjetas de crédito: En algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.

Llamadas internacionales: En algunas páginas, por lo general de material para adultos, se ofrece acceso gratuito a cambio de descargar un programa que en realidad desvía el módem a un número internacional o a un 906. La factura se incrementa notablemente en beneficio del propietario de la página.

Servicios gratuitos: Se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les ha cargado facturas a pesar de no haber pedido una prórroga en el servicio.

Ventas piramidales: Consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que éstos deben buscar.

Viajes y vacaciones: Determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.

Oportunidades de negocio: Convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera. En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.

Inversiones: Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.

Productos y servicios milagro: Algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

Mención especial merecen **"Las estafas del 906 en España".**

Pese a que el índice de uso del comercio electrónico entre los consumidores españoles es todavía muy bajo, las primeros indicios de fraude ya han hecho su aparición. Así, las principales quejas en España están relacionadas con el uso de números 906 a los que el usuario accede sin darse cuenta a través de páginas con contenidos pornográficos. 'Al usuario se le pide que acceda a seguir visualizando imágenes gratis, pero cuando presta su consentimiento para ello en realidad lo que está haciendo es acceder a un 906 con la consiguiente factura telefónica'. Miguel Pérez Subías, presidente de la Asociación de Usuarios de Internet (AUI).

Otra práctica habitual de los estafadores informáticos a través del servicio 906, es remitir a la víctima un e mail manifestándole que un supuesto pedido será recibido en su domicilio en fechas próximas, comunicando que de existir algún problema se ponga en contacto con un teléfono 906. Cuando la víctima lee el correo, y procede a llamar al teléfono de reclamaciones, se le mantiene largos minutos hasta que se le participa que se ha tratado de un error, con el consiguiente cargo a su factura telefónica[12]**.**

5.- DELITOS CONTRA LA PROPIEDAD INTELECTUAL

El ser humano es un ser creativo (aunque muchas veces también destructivo), es decir, es capaz de crear obras de artísticas, científicas, literarias, etc. En un principio, estas creaciones tenían "solo" un valor moral, pero conforme se fue avanzando en los tiempos se vio la necesidad de regular este sector, pues se daban al principio casos de plagio, para atribuirse una persona los méritos del trabajo de otra; pero además se llegó a un punto en el que todas estas obras tuvieron un valor patrimonial, valían dinero porque estaban en el comercio, las personas comerciaban, y comercian, con estas obras, con lo que era muy fácil el que una persona obtuviera beneficios económicos, por el trabajo intelectual de otra, sin autorización de esta última, que es su autor

[12] http://delitosinformaticos.com

original. Por todos estos motivos se vio la necesidad de proteger a los autores de estas obras, para que así se les reconociera socialmente por su trabajo, y además obtuvieran un beneficio patrimonial de ese trabajo, lo cual es totalmente legítimo. Por ello apareció el concepto de propiedad intelectual.

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

Según esta definición la propiedad intelectual se compone de un aspecto moral y otro patrimonial. Esta dimensión patrimonial la vemos reflejada en el art.270 CP, cuando hace referencia de forma expresa al ánimo de lucro del sujeto activo. Sin embargo, el contenido moral no aparece por ningún lado en el Código Penal, el cual se ve dañado cuando se realiza la conducta típica.

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

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

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

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

Especial referencia merece el tercer párrafo del art. 270 CP, ya que esta castigando expresamente la tenencia o fabricación de mecanismos que vulneren la protección de los programas informáticos, es decir, en base a este artículo es ilegal tener o fabricar programas para "crackear" otros programas. También se da mucho el caso de acceder a una página de esta índole y aparecer un mensaje de advertencia en el que se nos apercibe de la posible ilegalidad de tener en nuestra posesión estos programas, pero se nos exceptúa su ilegalidad en los casos en que se utilice con carácter educativo o investigador. Obviamente se puede alegar la eximente de ejercicio legítimo de un derecho, oficio o cargo -p. Ej. Si se es profesor de alguna rama relacionada, personal

investigador, etc.- regulado en el art. 20. 7º CP, por supuesto habrá que demostrarlo suficientemente, y que el Juez lo aprecie.

Como se desprende del art. 270 CP y de la Ley de propiedad intelectual, el medio que se utilice para realizar la conducta típica es indiferente, pues tanto en la Ley de propiedad intelectual, como en el Código Penal se nos dice que puede ser por "cualquier medio", y con ello quedan englobados tanto soportes físicos como digitales. Asimismo, objeto de propiedad intelectual puede ser cualquier obra original art. 10 LPI, por ejemplo, las fotografías, y por ello puede ser punible en base al art. 270 CP la venta de fotografías por personas no autorizadas por su titular. Como hemos dicho anteriormente, el ánimo de lucro es un elemento subjetivo del tipo, y sin el cual la conducta es atípica, y atípico sería el utilizar imágenes de cualquier sitio para ponerlas en tu página web, lo cual no quiere decir que no se pueda castigar en base a otros preceptos penales, civiles, o administrativos, siempre hay que atender a las circunstancias del caso concreto para determinar si se ha cometido una ilegalidad o no[13].

Relacionado con los delitos contra la propiedad intelectual haremos referencia a la copia de software sin ánimo de lucro, citando expresamente la sentencia de la **Audiencia Provincial de Barcelona, Sección 10ª, 10-6-1995,** (...) no toda vulneración o desconocimiento de los derechos derivados de la propiedad intelectual suponen sin más la realización de una conducta típica, y por ello, que no es suficiente con la realidad constatada de que el acusado con su conducta haya infringido lo dispuesto en el artículo 99.2 de la Ley de Propiedad Intelectual, en relación con la autorización del titular del derecho de explotación; porque no debe perderse de vista que el derecho de propiedad en cualquiera de sus manifestaciones goza de una protección tanto civil como penal, y esta última, por su naturaleza y circunstancias, debe actuar sólo con relación a los supuestos más graves de vulneración o desconocimiento del derecho. (...) El acusado tenía en su poder un número considerable de copias ilegales de programas, pero no hay constancia probatoria alguna de que hubiera realizado cualquier acto de tráfico o enajenación de los mismos ... de modo que lo único que le es imputable es la posesión que, aun cuando pueda vulnerar lo dispuesto en el artículo 99.2 de la Ley de Propiedad Intelectual, no entraña el tipo penal por el que se pretende la condena, que debe reservarse para supuestos más graves de vulneración y perjuicio de la propiedad intelectual, según antes se ha razonado[14].

---

[13] http://www.geocities.com

[14] Dr. Alejandro González Gómez, en su tesis doctoral dirigida por el Dr. D. Enrique Gimbernat Ordeig, titulada "el tipo básico de los delitos contra la propiedad intelectual.- De la reforma de 1987 al CP de 1995". Editorial Tecnos 1998

6.- DELITOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES.

La Constitución Española de 1978 protege el derecho a la intimidad en su art. 18.4 CE emplazando al legislador para que lo desarrolle con una Ley posterior, Ley de Protección de Datos (LPD). Aparte de esta Ley también el Código Penal protege la intimidad en el art. 197 CP. Pero antes de comenzar nuestro análisis de la intimidad la hemos de definir. La intimidad puede entenderse como la voluntad de una persona física o jurídica de que no sean conocidos determinados hechos que tan sólo ella o un número limitado de personas conoce (Muñoz Conde).

6.1.- La intimidad y las nuevas tecnologías en el Código Penal.

Como ya se ha venido afirmando a lo largo del presente trabajo, las nuevas tecnologías cada vez se van implantando más en nuestra sociedad, hasta el punto de que se ha hecho indispensable para determinadas tareas de vital importancia el uso de la informática y las telecomunicaciones, y además proporcionan un gran servicio a toda la sociedad. Pero como cualquier cosa en este mundo tiene sus aspectos negativos, y en este sentido la informática y las telecomunicaciones son utilizadas para atacar uno de los bienes fundamentales, constitucionalmente reconocidos, de cualquier persona: la intimidad. La informática se ha convertido en el medio propicio para atentar contra la intimidad de las personas, ya sea por simple altruismo (piénsese en los hackers, mal llamados piratas informáticos), o con fines lucrativos; de cualquiera de las dos formas la intimidad de una persona se ve afectada.

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

Por un lado, tenemos el art. 197.1 CP donde se contempla el tipo básico de descubrimiento de secretos, que consiste (como su denominación indica) en apoderarse de secretos para descubrir, sin una posterior divulgación o publicidad; con ello vemos que el delito se consuma simplemente con el apoderamiento para descubrir, aunque no se descubra nada (STS de 8 marzo de 1974). La jurisprudencia ha entendido por apoderamiento la aprehensión u obtención ilícita, así como la retención de lo recibido por error.

Como se deduce del propio art. 197.1 CP, ha de existir la finalidad de conocer algo reservado, el sujeto ha de apoderarse del secreto para descubrirlo, pero no de revelar, pues en dicho caso estaríamos ante la figura agravada del art. 197.4 CP.

Pero, ¿qué se entiende por secreto?, según Bajo Fernández, es "el conocimiento reservado a un número limitado de personas, y oculto a otras"; secreto será pues todo conocimiento reservado, que el sujeto activo no conozca, o no este seguro de conocer, y que el sujeto pasivo no quiera que se conozca; pero no hemos de confundir el secreto con el objeto en el que materializa, que puede ser un papel, una carta, mensajes de correo electrónico o cualquier otro documento personal.

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

El art. 197.1 CP, también regula la interceptación de las comunicaciones mediante "... artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación...". La pena que se prevé en art. 197.1 CP, es de uno a cuatro años de prisión, y multa de doce a veinticuatro meses.

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

Como podemos observar hay elemento subjetivo del tipo, que es "en perjuicio de tercero", donde "en" denota intencionalidad, y el perjuicio ha de interpretarse en sentido amplio, y por tanto no solo incluye los daños económicos.

Los datos personales o familiares han de estar registrados, esto es, contenidos, recogidos, anotados, transcritos, o grabados en "ficheros o soportes", y por tanto puede ser en un sistema informático, electrónico o telemático.

El último inciso hace referencia a "acceder por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero". Vemos que las conductas típicas son acceder, alterar o utilizar, pero ya no datos reservados, sino "ficheros o soportes informáticos, electrónicos, o telemáticos". En resumen este artículo castiga básicamente el "hacking", esto es, acceder a un sistema, sin estar autorizado para ello, y visualizar los datos de éste. Además se pueden dar otras conductas, como puede ser aprovecharse de esa información, y alterar, modificar, cambiar o vaciar la información que el sistema vulnerado contenía. La pena con que se sanciona estas conductas es prisión de uno a cuatro años, y multa de doce a veinticuatro meses, al igual que el art. 197.1 CP.

Pero el Código Penal no se queda ahí, además contiene una figura agravada (asigna una pena de dos a cinco años de prisión), recogida en el art. 197.3.1º CP, en la que además de realizarse la

conducta de apoderarse de un secreto, también se divulga ese secreto, con lo cual la vulneración de la intimidad es todavía más grave, y por ello el legislador ha penado esta conducta más gravemente. El concepto divulgación ha de entenderse como la comunicación a una o más personas de lo descubierto, incluso aunque estas personas no estén interesadas en su conocimiento. Por "revelar" hemos de entender el descubrir o manifestar el secreto. Por "ceder" se ha de entender transferir, o traspasar a otro una información.

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

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

Otra figura cualificada es la contenida en el art. 197.6 CP, donde se prevén penas superiores cuando las conductas descritas en el tipo básico se realicen con "ánimo de lucro", y a su vez distingue la punición dependiendo de si los datos son "sensibles" (art. 197.5 CP), o no lo son (párrafos del 1 al 4, del art. 197 CP); en el primer caso se prevé que se aplique una pena de cuatro a siete años, y en el segundo caso se prevé que se aplique al apena respectiva en su mitad superior. El ánimo de lucro se refiere a obtener una recompensa evaluable económicamente, con lo que su interpretación no plantea mayor dificultad.

Hay pocas sentencias relativas al nuevo artículo, salvo una de la Audiencia de Valladolid, que puede resultar muy ilustrativa.

> "El acusado, que prestaba sus servicios para la entidad denunciante asociación de parapléjicos y grandes minusválidos físicos, como conserje, merced a un acuerdo con los servicios de asistencia social de la prisión en la que se encontraba cumpliendo condena, en régimen abierto, sin disponer de autorización ninguna, o en todo caso, sin la de los responsables de prestarla, se apoderó de datos de carácter reservado, de índole personal

y familiar, registrados en soporte informático, de la asociación,mediante la toma de los disquetes que se encontraban en las oficinas, para copiar sus datos y transferirlos a su ordenador personal --en disco duro-- o, en otras ocasiones, mediante el acceso o lectura de referidos datos en su propio equipo informático,con un claro perjuicio, para los propios interesados o titulares de los datos --muy variados: domicilios, teléfonos, cuentas bancarias, estado y condiciones de salud física y mental, informes psicológicos, gastos, presupuestos, etc.-- y para la propia asociación, al acceder igualmente a su información reservada de administración y al verse quebrada la confianza y reserva puesta en ella por los socios; tales hechos son legalmente constitutivos de un delito de descubrimiento de secretos, previsto y penado en el art. 197 ps. 2, 5 y 6 [15].

[15] AP Valladolid, Sección 2ª. S. 14 de Julio de 1998. Ponente: Ilmo. Sr. San Millán Martín.

6.2.- REVELACION DE SECRETOS DE PARTICULARES COMETIDA POR FUNCIONARIO PUBLICO. ARTICULO 198 DEL CODIGO PENAL.

6.2.1.- Tipo objetivo

El delito es el mismo, si bien tiene un matiz distintivo que lo caracteriza: debe realizarlo un funcionario público, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo. En el supuesto de que se cometa en el curso de una investigación, ya no sería de aplicación este tipo penal, sino los previstos en los artículos 534 y siguientes, que como hemos dicho, no comporta el ingreso en prisión.

El objeto de este trabajo debería ser únicamente comentar el derecho positivo, pero es imposible evitar un juicio de valor. Pensemos en qué momento fue aprobado el Código Penal: varios funcionarios públicos estaban siendo investigados por haberse dedicado a realizar escuchas ilegales. Al penar más levemente a las fuerzas policiales en los casos que para perseguir delitos, se conviertan en hackers, el legislador dio carta de naturaleza al proyecto ENFOPOL.

6.2.2.- Tipo subjetivo

El autor del delito necesariamente ha de ser funcionario público, es un delito que no puede cometer un particular. La pena se ve agravada, pero pensemos que para evitar la aplicación de este artículo al autor del delito le bastará abrir un expediente, para de esa forma, tener la cobertura necesaria que justifique la escucha en el marco de una investigación. Creo que pocos preceptos penales se van a aplicar tan poco como éste.

6.3.- REVELACION DE SECRETOS DE EMPRESA. ART. 278 DEL C. PENAL

6.3.1.- Tipo objetivo

El delito es idéntico al previsto en el artículo 197, si bien deben tratarse de secretos de empresa. Obsérvese que aquí nos encontramos con una nueva discriminación: si alguien accede a un secreto de empresa, la pena mínima será de dos años de prisión; si el secreto es de un particular, sólo un año. Al parecer, son más importantes para el legislador las estrategias de venta de una multinacional que la última obra de un escritor, o el descubrimiento de un científico.

6.3.2.- Tipo subjetivo

Poco hay que añadir a lo que ya se ha dicho para artículos anteriores. El autor del delito puede ser tanto particular como funcionario, salvo que nos hallemos ante una investigación penal. Por el contrario, el sujeto pasivo necesariamente ha de ser una empresa, lo que entiendo será aplicable al comerciante individual.

7.- LOS DELITOS CONTRA LA PROPIEDAD INDUSTRIAL

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

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

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

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

Las conductas típicas que se describen en cada artículo no requieren mayor explicación, y basta con leerlos para comprender lo que en ellos se dice, pues, están bastante claros.

A la hora de interpretar el art. 275 CP hemos de tener presente lo que se dispone en la Ley 25/1970, Estatuto de la viña, el vino y los alcoholes, y los Reales Decretos 1573/1985, y 1396/1993, relativos a productos agroalimentarios.

En todos los tipos se prevé una pena de prisión de seis meses a dos años, y multa de seis a veinticuatro meses, para las conductas que verifiquen el tipo correspondiente.

Para terminar este análisis de la regulación jurídico-penal, haremos referencia a lo dispuesto en el art. 276 CP, esto es, la agravante que atiende al especial valor de los objetos producidos o a la especial importancia de los daños ocasionados. Si se da éste caso la pena asciende a prisión de dos a cuatro años, y multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con los delitos cometidos por un período de dos a cinco años[16].

8.- LA APOLOGIA DEL DELITO EN INTERNET

Internet se ha convertido en una " super autopista de información ", lo que se puede conseguir a través de ella es incalculable.

Pero es cierto que no todo lo que ofrece es válido, ya que muchas páginas web y portales ofrecen contenidos racistas, como es la propaganda nazi.

[16] http://www.geocities.com

Un tribunal francés otorgó a un famoso portal de Internet (Yahoo!) un periodo de tres meses para bloquear el acceso de los ciudadanos franceses a sus páginas norteamericanas que venden o exponen productos de simbología nazi.

Yahoo! cumplió con la ley francesa que prohíbe la venta y exposición de parafernalia nazi, pero esta sentencia obliga al portal a impedir que los franceses accedan a una página con sede en otro país. El tribunal francés pretende que Yahoo! utilice un mecanismo de bloqueo de acceso para los ciudadanos franceses.

Yahoo! también fue investigado por fiscales alemanes por distribuir copias del libro "Main Kampf " (Mi lucha) de Adolf Hitler (prohibido en Alemania) en subastas a través de su página en Internet.

Entre los productos que se ofertaban podemos señalar los siguientes:

Réplicas de frascos de gas, utilizados en los campos neonazis.

Insignias.

Uniformes.

Medallas.

Banderas .

Armas.

La venta de estos productos está prohibida en Alemania y en Francia.

Esta medida que propone el tribunal francés presenta un problema o inconveniente, y es que Yahoo! podría ser demandado en Estados Unidos por no respetar el derecho constitucional a la libertad de expresión. Incumple una ley nacional al acatar una decisión judicial de otro país.

Cada portal va a tener que adaptarse a la legislación de cada país si no quiere tener problemas, pero es una labor muy compleja, dado el gran número de legislaciones existentes y a la diversidad de las mismas.

Regular de forma unitaria Internet es muy difícil, ya que supondría unificar todos los criterios legales de todos los países en una sola legislación o marco legal.

La Comisión Europea va a permitir a los consumidores emprender acciones contra cualquier página europea de comercio electrónico en sus propios tribunales nacionales. Esta medida, conocida como la nueva Convención de Bruselas, podría permitir a los consumidores actuar contra empresas online con sede en el extranjero.

Por lo que respecta a nuestro sistema jurídico diremos que el artículo 18 del Código Penal define la apología como la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor. La apología sólo

será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito. En este sentido, el código penal castiga la apología de los siguientes delitos: homicidio y asesinato, lesiones, detenciones ilegales y secuestros, exhibicionismo y provocación sexual, robo, extorsión, estafa o apropiación indebida, receptación y otras conductas afines, cultivo y tráfico de drogas, rebelión militar, delitos contra la corona, asociación ilícita, sedición, atentados, terrorismo, y genocidio.

En la medida que sean utilizados medios informáticos para difundir las doctrinas que ensalzan el delito, la apología de delitos se convierte en delito informático, y en este sentido, son cada vez más numerosas las intervenciones frente a páginas Web que promocionan conductas delictivas como las mencionadas. Con todo, quiero insistir que se trata de un numerus clausus: sólo puede ser castigada como forma de provocación la apología de aquellos delitos para los que el código lo prevé.

La razón de ser de este delito está clara: la libertad de expresión no puede amparar la lesión de bienes jurídicos superiores. Cuando la libertad de expresión se convierte en un instrumento al servicio de los que atentan contra la vida y la libertad, debe actuar el derecho penal.

Incitación a la discriminación, odio y la violencia.

El artículo 510 del Código Penal castiga con prisión de uno a tres años y multa de seis a doce meses a aquellos que provocaren a la discriminación, al odio o a la violencia contra grupos o asociaciones, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia o raza, su origen nacional, su sexo, orientación sexual, enfermedad o minusvalía.

Serán castigados con la misma pena los que, con conocimiento de su falsedad o temerario desprecio hacia la verdad, difundieren informaciones injuriosas sobre grupos o asociaciones en relación a su ideología, religión o creencias, la pertenencia de sus miembros a una etnia o raza, su origen nacional, su sexo, orientación sexual, enfermedad o minusvalía.

Apología del genocidio y negación del holocausto.

Se trata de un delito que sólo se ha aplicado una vez en España, y no por Internet, sino frente al propietario de una librería que divulgaba libros que justificaban el nacionalsocialismo. El delito consiste en justificar actos de genocidio o negar el holocausto, previsto y penado en el artículo 607 CP, cuya acción perfectamente puede cometerse a través de la red.

Mención aparte merece la cuestión de la **apologia del hacking**

Para un sector de la doctrina no es delito elaborar y publicar una página Web en la que se haga apología del hacking. Y ello lo fundamentan porque, tal como establece el artículo 18 del Código penal, sólo puede penarse la apología cuando así se establece expresamente:

1. La provocación existe cuando directamente se incita por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante, que facilite la publicidad, o ante una concurrencia de personas, a la perpetración de un delito.

Es apología, a los efectos de este Código, la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor. La apología sólo será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito.

2. La provocación se castigará exclusivamente en los casos en que la Ley así lo prevea.

Si a la provocación hubiese seguido la perpetración del delito, se castigará como inducción.

No existe un precepto penal que establezca que la provocación o apología a cometer delitos de revelación de secretos o daños informáticos deba ser penada, a diferencia de lo que ocurre con delitos más graves, como homicidio y asesinato, lesiones, detenciones ilegales y secuestros, exhibicionismo y provocación sexual, robo, extorsión, estafa o apropiación indebida, receptación y otras conductas afines, cultivo y tráfico de drogas, rebelión militar, delitos contra la corona, asociación ilícita, sedición, atentados, terrorismo, y genocidio.

Apología es el elogio en abstracto de las acciones relativas al hacking, la consideración de los hackers como héroes de nuestro tiempo, que puede observarse en multitud de páginas presentes en la Red. Ello es algo completamente diferente de la inducción a cometer un delito concreto, que sí sería delito, si se diesen las condiciones establecidas por el Tribunal Supremo. Los requisitos de la inducción son, según sentencia de 5 de mayo de 1988:

1. Que la influencia del inductor ha de incidir sobre alguien que previamente no está decidido a cometer la infracción.
2. Que la incitación ha de ser intensa y adecuada, de forma que motive suficientemente al inducido a la perpetración del hecho deseado.
3. Que se determine a un ejecutor determinado y a la comisión de un delito concreto.
4. Que el inducido realice, efectivamente, el tipo delicitivo a que ha sido incitado.
5. Que el inductor haya actuado con la doble intención de provocar la decisión criminal y de que el crimen efectivamente se ejecute.

9.- LA PORNOGRAFIA INFANTIL

La pornografía en Internet es una de las fuentes económicas más prominentes, y que mueve más dinero que muchas multinacionales. La pornografía infantil vía Internet sigue creciendo pese a todos los esfuerzos realizados para erradicarla.

La mayoría de las páginas sexuales de Internet son muy difíciles de localizar y muchas de ellas están ligadas a los hackers, especialistas en evitar el rastreo mediante complejas operaciones de encriptación que borran su paso por la red.

En vista de que Internet no conoce ni reglas ni fronteras resulta imprescindible una mayor cooperación internacional.

Una persona puede registrar una web con contenido pornográfico en Argentina, por ejemplo, donde no hay legislación para el uso de Internet, y después cargarla desde cualquier parte del mundo.

Estos vacíos legales generan un crecimiento descontrolado y peligroso de este tipo de contenidos. Un sitio pornográfico, no necesariamente muestra que hay menores, se habla siempre de mayores de 18 años pero es difícil saber la edad realmente.

Los mayores productores de material pornográfico infantil son los países de Europa del Este y del este Asiático, donde apenas existe una legislación satisfactoria ni los medios técnicos necesarios para combatir este fenómeno. La mayoría de las fotos son de niños latinoamericanos, rusos y asiáticos. Las redes internacionales de pornografía infantil secuestran a niños, sobre todo de los orfanatos rusos para después realizar los vídeos pornográficos en los que se incluyen imágenes violentas, abusos y hasta asesinatos. Estas imágenes se vendían en vídeos a través de Internet y el precio oscilaba en función de lo escabroso de las imágenes.

Son numerosas las actuaciones policiales llevadas a cabo en todo el mundo para perseguir estos delitos. La policía Brasileña identificó algunos de los responsables de una red clandestina que divulgaba material pornográfico infantil en Internet, mediante programas de interceptación de e-mails.

Nuestro Código Penal en su artículo 189 establece que el que utilizare a un menor de edad o a un incapaz con fines exhibicionistas o pornográficos será castigado con la pena de prisión de uno a tres años.

En aplicación de citado precepto, y a título meramente informativo, citar que el día 10 de Octubre del 2000, la titular del Juzgado de Instrucción número 28 de Barcelona, abrió diligencias, por primera vez en España, contra un informático como presunto autor de la difusión de pornografía infantil a través de Internet. La juez imputa a este informático de 22 años el delito recogido en el artículo 189.b del Código Penal, castigado con penas de hasta 3 años de prisión. Este artículo fue introducido en el año 1998, dos años después de la entrada en vigor del texto, como respuesta a la proliferación de conductas de este tipo en Internet y el vacío legal existente hasta la fecha.

Por otro lado, en tanto en cuanto los Juzgados comiencen a depurar las responsabilidades penales por tales actuaciones, a modo de prevención la Unidad de Investigación de Delincuencia en Tecnologías de la Información (UIDTI) se ha puesto en contacto con todas las empresas

proveedoras de acceso a Internet (ISP) existentes en España, casi 1.700, para que eliminen los canales de distribución de material pornográfico, ya que muchos de estos proveedores no saben que las tienen, debido a la gran cantidad de páginas que albergan[17]

[17]Noelia García. http://delitosinformaticos.com
Carlos Sáncez Almeida. www.kriptopolis.com
www.bufetalmeida.com