

## **Caso Hispahack (1): Absolución de presuntos hackers. La sentencia**

28-05-1999

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 Policía 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 así 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 201.1 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 jurídico 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 aparecía un artículo atribuido a jfs, y tras realizar diversas gestiones lograron localizar en Internet 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 Internet 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 Internet, 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 afirmarlo 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 unase 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.