Caso Hispahack (2): Absolución de presuntos hackers. Informe final de la defensa

28-05-1999 por: Carlos Sánchez Almeida

INFORME FINAL DE LA DEFENSA: DESCRIMINALICEMOS LA RED

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.