Tribunal Supremo (Sala de lo Penal, Sección 1ª) Sentencia núm. 236/2008 de 9 mayo. Recurso de Casación núm. 1797/2007.

RESUMEN

El Tribunal Supremo considera que la policía judicial, cuando realiza rastreos en Internet, cumple con su función de perseguir delitos y detener a los delincuentes que los cometen, lo que tiene como consecuencia la validez de estos rastreos y la de las diligencias policiales practicadas en ejecución de autos autorizando la identificación de los usuarios de IPs y las diligencias judiciales de entrada y registro.

[…]

I. ANTECEDENTES DE HECHO

PRIMERO

El Juzgado de Instrucción núm. 5 de Tarragona incoó Procedimiento Abreviado con el número 97/2006 contra Ángela, y una vez concluso se remitió a la Audiencia Provincial de Tarragona, cuya Sección Cuarta, con fecha dos de mayo de dos mil siete dictó sentencia que contiene los siguientes HECHOS PROBADOS:

"a) Sobre la obtención de las fuentes de prueba.

Con fecha 25 de octubre de 2005 tuvo entrada en el Juzgado de Instrucción número 7 de Sevilla comunicación escrita del Grupo de Delitos Telemáticos de la Policía Judicial de la Guardia Civil en la que se exponía que aprovechando la celebración en Sevilla del IV Foro Iberoamericano de Ciberpolicías, dicho grupo policial había iniciado el día 22 de octubre de 2005 y tenía previsto realizar hasta el día 28 de ese mismo mes, búsquedas en Internet rastreando las redes de intercambio de archivos (Peer to Peer), para averiguar aquellos usuarios que descargasen o compartiesen entre dichas fechas archivos conteniendo fotografías o vídeos con contenido de pornografía infantil que previamente habían identificado e incluido en sus bases de datos.

Con carácter previo a dichos rastreos, ese grupo policial había creado una base de datos formada por 1.000 archivos de fotografías y vídeos con contenidos de pornografía infantil identificados de forma electrónica mediante su número "hash" con independencia del nombre que pueda asignarle en cada momento el usuario que es enteramente mudable.

En base a dichos rastreos policiales, realizados sin ningún tipo de autorización judicial, obtuvo dicho cuerpo policial un listado de "IPs (Internet Protocols)", esto es, claves de acceso que los Proveedores de Servicios de Internet asignan a cada ordenador en el momento en el que se conecta a Internet, el cual permite identificar de forma indubitada a través de dichos Proveedores el número telefónico desde el que se produce la conexión. Dicho listado de "IPs" obtenido por el cuerpo policial comprendía aquellos accesos a internet que se habían producido entre los días 22 a 29 de octubre de 2005, a través de los cuales se habían efectuado descargas o intercambios de los archivos cuyo número "hash" había sido incluido previamente en la base de datos creada por el Grupo de Delitos Telemáticos, identificando en dichos listados, las "IPs" concretas de cada

conexión, los archivos concretos transmitidos desde cada una de ellas, así como las horas a las que se habían producido.

Dicho listado se presentó con posterioridad en el Juzgado de Instrucción número 7 de Sevilla, solicitando emisión de mandamiento judicial dirigido a los diferentes proveedores de servicios de internet existentes en España para que identificasen al titular, domicilio, número de teléfono y forma de pago correspondiente a cada uno de los "IPs" que habían identificado en sus rastreos. En cumplimiento de dicho mandamiento judicial se obtuvo que la acusada Ángela había utilizado los accesos a internet correspondientes a los números IP NUM000 y NUM001 incluidas en dicho listado.

En base a dicha información se acordó por el Juzgado de Instrucción núm. 7 de Sevilla la entrada y registro en el domicilio de la acusada sito en el PASEO000 núm. NUM002 de la Pineda (Tarragona), que se efectuó el día 21 de febrero de 2006, en el que se intervino y analizó el contenido del ordenador personal que allí hallaron.

b) Sobre los hechos por los que se formula acusación:

La grave lesión al derecho fundamental al secreto de las comunicaciones en la obtención del material probatorio impide estimar acreditado que la acusada haya efectuado descarga alguna o acto de difusión de archivos con contenido de pornografía infantil, viciando de ilicitud al resultado del registrado del ordenador personal de la acusada, quedando tan sólo acreditado:

La acusada Ángela era usuaria del sistema de intercambio de archivos Emule del cual se servía para obtener la descarga de archivos de fotografía, música o películas, cuya selección efectuaba introduciendo palabras clave que pudieran aparecer en el título que otros usuarios habían asignado a los archivos que ponían a disposición de otros posibles usuarios para compartir. El propio sistema de intercambio de archivos no verifica que el contenido de cada archivo responda al título mudable que cada usuario pueda asignarle en cada momento, de tal forma que en ocasiones un título inocuo puede resultar con un contenido diferente al que en un principio pudiera sugerir el título con el que se selecciona la descarga, o incluso contener material pornográfico. El contenido únicamente puede ser averiguado a través de su visualización por el usuario que solicita la descarga una vez obtenida la descarga parcial o total del archivo, si bien incluso antes de dicha comprobación o incluso aunque ésta no se lleve a cabo, el propio archivo o las fracciones del mismo que ya se han descargado son a su vez compartidas de forma automática con otros usuarios del sistema.

En suma, un mismo archivo, identificado de forma electrónica mediante su número "hash" puede aparecer ofertado por diferentes usuarios bajo títulos diferentes, variables en cada momento, de la misma forma que un mismo título puede responder a contenidos diferentes.

En algunas ocasiones, meses antes de la entrada y registro efectuada en febrero de 2006, la acusada realizó búsquedas de archivos a través de títulos que contuvieran las palabras "bebés", "mamás", "papás", "niñas", "girls", "boys", "mamas con bebes", sin que quede acreditado que pretendiera obtener a través de dichas búsquedas archivos que contuvieran pornografía infantil. En varias ocasiones los archivos así descargados, resultaron contener pornografía infantil que la acusada borraba de su ordenador".

SEGUNDO

La Audiencia de instancia dictó el siguiente pronunciamiento:

"Que debemos ABSOLVER Y ABSOLVEMOS a Ángela del delito de facilitación de la difusión de material de pornografía infantil, previsto y penado en el art. 189 C.P, declarando de oficio las costas causadas en esta instancia.

Notifíquese esta resolución a las partes".

TERCERO

Notificada la sentencia a las partes, se preparó recurso de casación por infracción de Ley y de precepto constitucional, por el MINISTERIO FISCAL […]

CUARTO

El recurso interpuesto por el MINISTERIO FISCAL se basó en el siguiente MOTIVO DE CASACIÓN: Único.- Al amparo del art. 852 de la Ley Enj. Criminal por infracción del art. 24 y 18.3 de la C.E articula el presente recurso por infracción del derecho a la tutela judicial efectiva en relación con el derecho a la prueba por cuanto la Audiencia dictó sentencia absolutoria tras declarar la nulidad de la prueba en que se sustentaba la acusación del Ministerio Fiscal, por estimar vulnerado el derecho al secreto de las comunicaciones.[…]

II. FUNDAMENTOS DE DERECHO DE INTERÉS

PRIMERO

Al amparo del art. 852 L.E.Cr. el Ministerio Fiscal en motivo único se alza contra la sentencia absolutoria recaída en esta causa por entender infringidos los arts. 24-1 y 18-3 C.E.

1. La sentencia declara la nulidad de la prueba (derecho a la prueba) que constituía el sustento de la imputación acusatoria del Fiscal y declara probado que el Grupo de Delitos Telemáticos de la Policía Judicial de la Guardia Civil, realizó búsquedas en Internet rastreando las redes de intercambio de archivos (Peer to Peer) para averiguar aquellos usuarios que descargasen o compartiesen archivos conteniendo fotografias o vídeos con contenido de pornografía infantil. En base a dichos rastreos policiales, realizados sin autorización judicial, se obtuvo un listado de IPS (Internet Protocols), esto es, claves de acceso que los proveedores de servicios de Internet asignan a cada ordenador en el momento en el que se conecta a Internet, el cual permite identificar de forma indubitada a través de dichos proveedores el número telefónico desde el que se produce la conexión.

2. El Fiscal entiende que la sentencia parte de unas premisas equivocadas y monta su argumentación sobre los siguientes pilares:

a) A su juicio yerra la sentencia al afirmar que la Guardia Civil tuvo acceso, sin autorización judicial, a datos confidenciales de la acusada "preservados del conocimiento público y general", lo que no es enteramente cierto, ya que no hay secreto

sobre datos que el partícipe en la comunicación informática voluntariamente aporta a la red de redes.

b) Mediante la utilización de un programa P2P no se afecta el derecho fundamental al secreto de las comunicaciones. Lo que se averigua por la Guardia Civil en los rastreos efectuados es qué IPS habían accedido a los "Hash" que contenían pornografía infantil. A esa información, que es la única que se obtiene sin autorización judicial, puede acceder cualquier usuario de la red. La huella de la entrada, el IP, queda registrado siempre y ello lo sabe el usuario.

c) Consecuentemente la Audiencia confunde -en opinión del Mº Público- las comunicaciones telefónicas tradicionales con el acceso telefónico a Internet, sus reglas, requisitos y efectos. Reconoce que la doctrina jurídica contenida en las sentencias que la fundamentación jurídica de la recurrida cita es correcta, siempre que se refieran a comunicaciones estrictamente telefónicas. En este sentido realiza las siguientes matizaciones:

-en la telefonía convencional los números desde donde se efectúan o reciben las llamadas se hallan protegidos por el derecho al secreto de las comunicaciones (S.T.E.D.H.: caso Malone de 2-agosto-1984); sin embargo en las comunicaciones por Internet el teléfono es un mero instrumento de comunicación con la red.

-de ahí que quien utiliza voluntariamente un programa (Peer to Peer: P2P), en nuestro caso EMULE, asume y consiente que muchos de los datos que incorpora a la red pasen a ser de conocimiento público para cualquier usuario de Internet.

-a su vez las claves identificativas (Internet Protocols: IPs) no concretan a la persona del usuario, sino sólo el ordenador que se ha usado, lo que hace necesario para poder llegar a conocimiento del número de teléfono y titular del contrato (datos que pueden reputarse reservados) la autorización judicial, que es lo que se hizo en el caso que nos ocupa ante el Juzgado de Instrucción núm. 7 de Sevilla que expidió el correspondiente mandamiento.

-así las cosas es visto que los rastreos policiales previos que se tildan de ilegales, sólo afectaban a datos públicos de Internet no protegidos por el art. 18-1º y 3º de la Constitución y en consecuencia las pruebas obtenidas y las derivadas no se hallaban afectas a vicio alguno.

3. Planteado así el problema, se hace preciso o cuando menos conveniente esbozar un esquema de los criterios legales y jurisprudenciales en orden a la calificación de la actuación policial de acuerdo con la legalidad procesal y constitucional.

En este sentido y en cuanto al alcance del contenido del derecho al secreto de las comunicaciones previsto en el art. 18-3 C.E., la sentencia recurrida concreta acertadamente su contenido material, circunstancia que concuerda con las tesis del Fiscal recurrente.

Desde la sentencia del Tribunal Constitucional núm. 123 de 20 de mayo de 2002, se establece, haciéndose eco del caso Malone (2-8-84), resuelto por el Tribunal de Estrasburgo de Derechos Humanos, que la obtención del listado de llamadas hechas por los usuarios mediante el mecanismo técnico utilizado por las compañías telefónicas

constituye una injerencia en el derecho fundamental al secreto de las comunicaciones reconocido en el art. 8 del Convenio Europeo, equivalente al 18-3 C.E. En cuanto al concepto de secreto de la comunicación no sólo cubre su contenido, sino otros aspectos de la comunicación, como la identidad subjetiva de los interlocutores. Consecuentemente podemos afirmar que el secreto a las comunicaciones telefónicas garantiza también la confidencialidad de los comunicantes, esto es, alcanzaría no sólo al secreto de la existencia de la comunicación misma y el contenido de lo comunicado, sino a la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino". Hasta este nivel discursivo existe coincidencia entre la posición del tribunal de instancia y el Mº Fiscal.

También cita la sentencia combatida la de esta Sala núm. 130 de 19 de febrero de 2007, por resultar oportuna dados los temas tratados, próximos al problema a discernir ahora. En dicha sentencia, completada por un voto particular de dos magistrados, también existía coincidencia en orden a insertar dentro del derecho al secreto de las comunicaciones todo lo referente al desvelamiento de los interlocutores de una conversación telefónica, así como el día, hora y duración de la misma, aunque no se haya interferido en el contenido de la comunicación.

El problema se suscitaba en la averiguación del número de teléfono o identidad del usuario de un determinado número. Usualmente, la policía judicial cuando interesa una actuación injerencial del juez, concreta y precisa los números telefónicos que deben ser intervenidos, incluso facilitando sus titulares o posibles usuarios, que coinciden con las sospechas sobre las mismos de estar cometiendo algún delito.

En el voto particular no se califica de injerencia ilegítima la simple averiguación de los números telefónicos usados por una persona, en cuanto no contravendría la doctrina del caso Malone ni la de nuestro Tribunal Constitucional, ya que sería preciso para merecer protección que se indagara (cosa que en el caso resuelto por la sentencia de 2007 no ocurre) el teléfono o la persona destinataria de la llamada, así como el momento y duración de la conversación mantenida.

La sentencia de 2007, en su voto reservado, siguiendo una línea doctrinal de esta Sala, acorde con la sentada por el Tribunal Constitucional, justifica el conocimiento por parte de la policía judicial del número telefónico perteneciente a una persona, por informaciones confidenciales, listines telefónicos, registros o documentos públicos o privados, etc.

Dicha sentencia, sin embargo, sin contradecir tal observación entiende con fundamento que necesariamente se debió intervenir una conversación para conocer dicho número, habida cuenta de los testimonios policiales que aludían a la utilización de un artilugio técnico para la obtención del dato.

4. Queda en pie la duda, de si para solicitar el número telefónico o identidad de una terminal telefónica (cabría extenderlo a una dirección o identificación de Internet: Internet protocols), es necesario acudir a la autorización judicial, si no han sido positivas las actuaciones policiales legítimas integradas por injerencias leves y proporcionadas, que puede respaldar la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado o Ley de Seguridad Ciudadana, en la misión de los agentes de descubrir delitos y perseguir a los delincuentes.

A nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina (obiter dicta), los datos identificativos de un titular o de una terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18-3 C.E.) sino en el marco del derecho a la intimidad personal (art. 18.1º C.E.) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal, LO 15/1999 de 13 de diciembre: art. 11.2 d. o su Reglamento, Real - Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, RD 424 de 15 de abril de 2005, en los que parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal.

Tampoco debe pasar por alto, aunque sólo sea con carácter dialéctico, el contenido de la Ley núm. 25 de 18 de octubre de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, que al igual que el Reglamento de la Ley de protección de datos son posteriores a los hechos aquí enjuiciados y por ende no aplicables.

La Ley últimamente citada que se dicta en desarrollo de la Directiva de la Unión Europea 2006-24 - C.E. del Parlamento Europeo y del Consejo de 15 de marzo del mismo año tiene por objeto imponer la obligación a los operadores de Telecomuniaciones de retener determinados datos generados o tratados por los mismos con el fin de entregarlos a los agentes facultados, en caso de que le fueran requeridos por éstos, entendiendo por tales agentes los pertenecientes a los Cuerpos policiales, al Centro Nacional de Inteligencia y a la Dirección de Vigilancia aduanera. Esta Ley exige para la cesión de estos datos, con carácter general, la autorización judicial previa y entre los datos que deben conservar figura el que es objeto del proceso que nos ocupa (los datos que deben ser custodiados por los operadores de telecomunicaciones están ampliamente descritos en su art. 3º).

SEGUNDO

Visto el panorama jurisprudencial y legislativo y trasponiéndolo al caso que nos ocupa se puede concluir lo siguiente:

a) **los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma.** La huella de la entrada -como puntualiza con razón el Mº Fiscal- queda registrada siempre y ello lo sabe el usuario.

b) entender que **conforme a la legalidad antes citada (unas normas vigentes en el momento de los hechos y otras posteriores) se hacía preciso acudir a la autorización del juez instructor para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data).** La policía judicial a través de un oficio de 6 de noviembre de 2005, completado por un informe de 24 de octubre del mismo año del

Grupo de delitos telemáticos de la Guardia Civil interesa la preceptiva autorización que obtuvo con el libramiento de mandamiento judicial dirigido a los operadores de Internet para identificar ciertas direcciones IP del ordenador al objeto de proseguir la investigación.

Consecuentemente quien utiliza un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en internet, no se hallaban protegidos por el art. 18-1º ni por el 18-3 C.E.

TERCERO

Por todo ello debe quedar patente que al verificar los rastreos la policía judicial estaba cumpliendo con su función de perseguir delitos y detener a los delincuentes que los cometen, siendo legítimos y regulares los rastreos efectuados, lo que trae como consecuencia la validez de los mismos y la de las diligencias policiales practicadas en ejecución del auto autorizando la identificación de los usuarios de IPs y el posterior de entrada y registro, determinando la nulidad de la sentencia que el Fiscal interesa.

Ello no empece, fijándonos en el segundo apartado de hechos probados y fundamentación jurídica a este particular referida, que a pesar de la validez de las pruebas indebidamente expulsadas del proceso, concurrieron en el caso otros elementos probatorios, capaces -quizás- de excluir la culpabilidad de la acusada. Pero ese punto no se cuestiona ni recurre.

Por consiguiente, la nulidad de la sentencia obligará al mismo Tribunal a dictar otra en el que se considere dentro del acervo probatorio todas las actuaciones, diligencias y pruebas practicadas en la causa que se han declarado nulas en la combatida y las que de ellas traen causa, para que en valoración conjunta con las demás practicadas dicten nueva sentencia, condenado o absolviendo, según proceda en derecho. […]

III. FALLO

Que debemos DECLARAR Y DECLARAMOS HABER LUGAR al recurso interpuesto por el MINISTERIO FISCAL, por estimación del único motivo articulado, declarando NULA LA SENTENCIA dictada por la Audiencia Provincial de Tarragona, Sección Cuarta, procediendo por la misma Sala a dictar otra, en la que se tenga en consideración como pruebas legítimas las declaradas nulas por el Tribunal y las que de ellas deriven, valorándolas en conjunción con el resto del elenco probatorio válido. […]