Abril de 2010

DETENIDOS P2P

ORIENTACIONES PARA EL ABOGADO DEFENSOR

Características del delito atribuido al detenido P2P

Estimado abogado, su cliente ha sido detenido en una redada P2P motivada por el delito de **difusión o facilitación intencionada de pornografía infantil**, castigada en el artículo 189.1.B del código penal español.

Un delito perseguido de oficio por los agentes, mediante procesos de rastreo **sin control judicial, realizados con programas informáticos no homologados**.

Este delito requiere para ser tipificado de la existencia de ambos componente, objetivo y subjetivo. El componente objetivo es **técnico**, concretado en la acción medible de difundir o facilitar. El componente subjetivo es **psicológico**, concretado en el dolo que debe ser acreditado según la doctrina del Tribunal Supremo, que más adelante le detallo.

A raíz de esta detención, y en base a los resultados posteriores de la revisión de los equipos del detenido, a su cliente podrían imputarle el delito de **tenencia para uso propio** contemplado en el artículo 189.2 del código penal.

De igual manera, este artículo requiere el componente subjetivo, ya que debe acreditarse la tenencia para "uso propio".

En ocasiones los fiscales, atendiendo al grado de execrablilidad, suelen solicitar los agravantes del 189.1.3 o la aplicación del artículo 74 de delito continuado. El Tribunal Supremo ya ha aclarado en reiteradas ocasiones la no aplicabilidad de estos agravantes en los casos de detenidos P2P.

Artículo 189.1.b y el tipo objetivo

Son numerosos los casos dónde el delito (difundir o facilitar + intención) se tipifica por la **autoinculpación** en su declaración del detenido P2P y no por las pruebas técnicas o psicológicas aportadas por los investigadores.

El interrogatorio policial está cargado de preguntas capciosas en busca del dolo (aunque sea eventual).

Debe saber que las redes P2P están plagadas de archivos denominados **fakes files** (archivos cuyo nombre no hace referencia a su contenido). También existen los **ficheros clones** (archivos con similar identificador HASH con contenidos distintos).

Los agentes reciben diariamente cientos de notificaciones anónimas de usuarios P2P que se tropiezan con estos execrables contenidos. Generalmente estas denuncias originan las operaciones P2P, que suelen culminar con detenciones masivas de internautas que pudieran estar en similar situación que los internautas denunciantes.

Por tanto, ante una pregunta del tipo ¿se ha descargado usted alguna vez pornografía infantil de la red P2P? Cabe la probabilidad de que el detenido hubiera padecido en el pasado un tropiezo accidental con estos lamentables contenidos.

Otra pregunta típica en los interrogatorios policiales ¿sabe usted que al descargar un archivo de la red P2P lo está poniendo a disposición de otros usuarios? No hay que ser un experto informático para saberlo, así que muchos usuarios contestan afirmativamente. El Fiscal ya tendría los elementos para conformar el dolo (al menos eventual).

La carga emocional que conlleva ser detenido por estos asuntos, facilita la aparición en el detenido de **sentimientos de culpa** frente a una situación del todo inexplicable, incluso para sí mismo.

SUGERENCIA: Es recomendable que su defendido **no declarase contra sí mismo**, tal y como garantiza nuestra Constitución.

Entonces ¿Cómo podría la Fiscalía conformar el tipo objetivo para certificar que se ha facilitado o difundido?

La **única prueba técnica posible** sería la revisión posterior del registro de actividad del cliente P2P utilizado por el internauta. En el caso del eMule, la caja negra se haya en el archivo **Known.met** (conocidos). En este archivo se guarda una línea por cada archivo que ha pasado por ese eMule. Uno de los campos de esa línea hace mención a los **Bytes Difundidos**, que no es otra cosa que el registro de la **medición de la difusión** de ese archivo concreto.

Posiblemente llegados a este punto se esté preguntando: entonces ¿cómo es posible que la policía esté tan segura que mi defendido difundió? La respuesta es algo alarmante. El **criterio policial es erróneo** ya que parte de una premisa técnica errónea: Técnicamente **la IP externa no identifica al infractor P2P, sino al titular de la conexión**.

Es muy fácil de entender: Detrás de una IP externa o pública puede existir uno o varios ordenadores, uno o varios usuarios, uno o varios eMule, un extraño conectado a la Wifi del detenido, un troyano instalado en su ordenador compartiendo porno infantil, una descarga accidental, etc. Por tanto la IP externa, facilitada puntualmente por el proveedor de internet, es un indicio insuficiente como para ordenar un registro domiciliario.

Artículo 189.1.b y el tipo subjetivo

Como le he indicado en el apartado anterior, son numerosos los casos en los que este delito se tipifica en base a la declaración del detenido y no en base a las pruebas técnicas halladas.

Una vez fundamentado el tipo objetivo, el Tribunal Supremo establece las pautas para determinar el dolo. En acuerdo de 27 de octubre de 2009 sobre facilitamiento de la difusión de la pornografía infantil (alcance del art. 189.1.B) del C Penal, el TS dice lo siguiente:

> Acuerdo:
> Una vez establecido el tipo objetivo del art.189.1.b) del C.Penal, el subjetivo deberá ser considerado en cada caso, evitando incurrir en automatismos derivados del mero uso del programa informático empleado para descargar los archivos.
>
> Eduardo de URBANO CASTRILLO

Las pautas para determinar el dolo en los casos P2P, según el TS, son las siguientes:

STS 964/2010 - STS 7211/2009 - STS 236/2009

> …cuando se trata de una acción de compartir archivos recibidos, tal dolo se ha de inducir del número de elementos que son puestos en la red a disposición de terceros , para lo que se tendrá en cuenta la estructura hallada en la terminal (archivos alojados en el disco o discos duros, u otros dispositivos de almacenamiento), el número de veces que son compartidos (pues este parámetro deja huella o rastro en el sistema informático), la recepción por otros usuarios de tales imágenes o vídeos como procedentes del terminal del autor del delito, y cuantas circunstancias externas sean determinadas para llegar a la convicción de que tal autor es consciente de su actividad de facilitar la difusión de pornografía infantil, entre las que se tomará el grado de conocimiento de la utilización de sistemas informáticos que tenga el autor del delito.

Por tanto y siguiendo esa doctrina pasamos a responder a esas cuestiones.

¿Cuántos elementos fueron puestos a disposición de terceros?

Indica además el TS que se tendrá en cuenta lo siguiente:

Estructura hallada en la terminal

Este dato parece obvio ¿cuántos archivos de pornografía infantil han sido hallados en los dispositivos del detenido?

La realidad es más complicada de lo que parece. En muchas ocasiones, el rastro P2P del archivo investigado si quiera aparece.

Por otro lado, generalmente todos pensamos que a simple vista, podríamos determinar si una imagen corresponde a un infante o no. El problema surge cuando la imagen está protagonizada por personas en la **franja de edad de la incertidumbre**. La ley castiga cualquier imagen pornográfica de un menor de 18 años ¿pero existe algún

procedimiento científico que acredite con la simple estimación visual la edad de una persona joven? La respuesta es un rotundo ¡No! Recordemos el caso del pirata somalí. Ni teniéndolo de cuerpo presente, fue científicamente imposible determinar su edad con exactitud.

En ocasiones, los agentes utilizan una herramienta informática denominada **Perkeo**.[1] Este software elaborado por un ciudadano alemán, al instalarlo en un PC permite localizar archivos de **pornografía infantil o de animales**, emitiendo un informe de los resultados. Un software no homologado para tal fin por ninguna entidad certificadora, por lo que es altamente recomendable solicitar la visualización de los archivos catalogados como ilegales por esta aplicación.

El número de veces que son compartidos

Este dato es técnicamente confuso (*). En cualquier caso únicamente puede obtenerse del análisis del registro de actividad del programa de intercambio de archivos. En el caso del eMule, este registro se encuentra en el archivo Known.met (conocidos). El proceso para obtener este dato sería localizar en el registro del eMule, todas aquellas filas que contuvieran:

1) Un **Hash de archivo** identificado como contenido ilegal.
2) Un **nombre de archivo en español** con referencia explícita a pornografía infantil.
3) Un valor > 0 en la **columna Bytes difundidos** que determinar la difusión efectiva. (*) Posiblemente estará pensando que el número de veces que un archivo ha sido difundido se puede calcular dividiendo este valor (Bytes difundidos) entre el tamaño del archivo (indicado en la columna correspondiente). Pues ¡no! Un archivo en la red P2P se comparte por partes denominadas "chunk" de 9Mb. que han podido ser independientemente difundidas con mayor o menor acierto ¿Se podría determinar entonces si el archivo ha sido enviado al completo a un tercero en algún momento? ¡No!. Técnicamente es un dato incontestable y no se puede determinar en este punto de la investigación.

   Quizás el momento para contar al menos una difusión efectiva desde la IP del detenido, debió realizarse en el rastreo P2P inicial de los agentes ¿Recibió el rastreador P2P policial alguna parte del archivo desde la IP del detenido? Posiblemente no se indique nada al respecto.

Error de interpretación técnica: El error consiste en interpretar los valores almacenados en los campos "Peticiones recibidas" y/o "Peticiones aceptadas" del

[1] http://www.perkeo.net/

registro del eMule Known.met, como "el número de veces que es compartido un determinado archivo"[2]

La recepción por otros usuarios de tales imágenes o vídeos como procedentes del terminal del autor del delito

Otro dato imposible de hallar. Para comprender por qué, es necesario explicar cómo se inicia el procedimiento policial. Aunque pueden existir diferencias entre el número de rastros empleados, este sería el procedimiento básico:

1) Un internauta se tropieza con un archivo de pornografía infantil y lo denuncia a los agentes indicando el nombre o el HASH del archivo.
2) Los agentes con programas convencionales se descargan de la red P2P ese archivo para comprobar que efectivamente se trata de pornografía infantil. Nótese que en este punto los agentes pudieran estar cometiendo el mismo delito que persiguen.
3) Una vez descargado y comprobado su contenido ilegal, se realiza nuevamente la descarga y se hacen impresiones de pantalla donde se muestra los datos básicos de la fuente P2P (IP externa o pública + nombre execrable).
4) Se justifica a un juez la gravedad del delito para que autorice a la identificación del titular de la IP externa o pública en se momento.
5) Una vez identificado, y **sin mediar ningún tipo de investigación convencional**, se solicita judicialmente la orden de entrada y registro del titular de la conexión.

El proceso anterior corresponde a la investigación de un archivo en un momento determinado empleado por la BIT en el año 2006.[3]

Nótese que los agentes no tienen capacidad de administrar la red P2P. Su investigación se realiza desde un extremo o PEER (igual), con una aplicación P2P convencional, como si de un internauta convencional se tratara. Tanto es así, que el rastreo P2P se realiza sin control judicial y en ocasiones con rastreos P2P realizados fuera de España (p.e: operación Carrusel y Ruleta).

[2] http://www.lawp2p.com/indignado77/FalseQueueRank.pps
[3] http://www.lawp2p.com/indignado77/bazooka.pdf

Y cuantas circunstancias externas sean determinadas para llegar a la convicción de que tal autor es consciente de su actividad de facilitar la difusión de pornografía infantil, entre las que se tomará el grado de conocimiento de la utilización de sistemas informáticos que tenga el autor del delito.

Utilizar como agravante el grado de conocimientos informáticos o de inglés que pudiera tener el detenido suena a tiempos pasados, en los que saber era castigado con la hoguera. Existe una gran diferencia entre **tener conocimientos** sobre una materia a **tener conciencia** de que un delito se está cometiendo.

Es importante señalar que los clientes P2P como el eMule funcionan de forma desatendida. Un usuario puede iniciar la descargar de numerosos archivos y comprobar si han sido recibidos días después.

También debemos recalcar que la opción de previsualización de un archivo antes de completar su descarga no es siempre factible. Se requiere tener descargadas al menos la primera y última parte (chunk de 9Mb) del archivo.

Como hemos mencionado antes, las redes P2P están llenas de archivos falsos. Ni los más expertos están a salvo de realizar una descarga accidental.

Para cualquier consulta, duda o rectificación, puede contactar conmigo:

Indignado7777@gmail.com