

Procesal Penal - España

30/09/2015 15:26:41 | Prueba electrónica

Las contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo

Ana Isabel Betrán Pardo - Fiscal sustituta. Licenciada en Criminología

Los avances tecnológicos nos sitúan ante la presencia en el proceso penal documentos electrónicos como son los derivados de aplicaciones de mensajería instantánea como WhatsApp, cuya aportación es frecuente en las diligencias urgentes. La reciente STS 300/2015, de 19 de mayo, advierte de las cautelas con que ha de ser abordada la prueba de una comunicación bidireccional, dadas las posibilidades de manipulación de los archivos, por lo que considera indispensable que se practique una prueba pericial en caso de que la documental sea impugnada. No obstante, la práctica de esta pericial está rodeada de numerosos obstáculos de muy diversa naturaleza.

1. Planteamiento de la cuestiones objeto de análisis

Las nuevas tecnologías generan nuevos tipos de documentos que hasta hace poco tiempo resultaban extraños al marco procedimental penal, consecuencia de lo cual, no puede obviarse que en los últimos años el modo de comunicarse de las personas ha sufrido un cambio sustancial. No sólo se encuentran en desuso las clásicas cartas sino que también puede observarse que el uso del teléfono móvil, únicamente como medio de establecer conversaciones, ha disminuido de forma directamente proporcional a la aparición de otras formas de comunicación que resultan posibles a través de un terminal telefónico. En efecto, los conocidos como smartphones mediante su conexión a Internet han propiciado el desarrollo de aplicaciones de mensajería instantánea que son masivamente utilizadas para establecer comunicaciones bidireccionales o multidireccionales entre personas. Y este acontecimiento social derivado del uso de las nuevas posibilidades tecnológicas afecta en general a la ciencia jurídica y en particular, y en lo que nos afecta, al derecho penal, pues se plantea el reto de verificar a través de qué forma van a introducirse estos mensajes, así como los demás archivos que se generan en el concreto marco procedimental de la LECrim.

Una de estas aplicaciones de mensajería, que además es la más utilizada en el mundo, es la conocida como WhatsApp y en torno a la misma aparecen algunas cuestiones que han de ser analizadas debido a su trascendencia, pues si bien entre las bondades de esta forma de comunicación pueden predicarse su alto grado de practicidad, rapidez y comodidad, no puede olvidarse que como todas las comunicaciones electrónicas ésta tampoco queda al margen de que determinadas personas puedan hacer un uso indebido de la misma, pues puede ser fácilmente manipulable, lo que nos sitúa ante la necesidad de cuestionar su validez y eficacia, dado que además la característica particular de esta aplicación es que el administrador no conserva el contenido de las conversaciones, sino sólo ciertos datos de tráfico relacionados con las comunicaciones.

Al hilo de lo que se acaba de exponer, la reciente Sentencia de la Sala II del Tribunal Supremo número 300/2015, de 19 de mayo, analiza el tema de la facilidad de manipulación de este tipo de pruebas,

indicando que lo anterior implica la necesidad de ser objeto de prueba pericial en el caso de que sea impugnada, correspondiendo esta carga probatoria a quien pretende hacerla valer. Se trata de una doctrina de una gran trascendencia para el proceso penal ya que no resulta extraño, que la praxis diaria de un Juzgado de Violencia de Género o de Instrucción en funciones de guardia, nos sitúe ante la posibilidad de contar como medio probatorio con los contenidos de mensajería instantánea aportados por la víctima de los que pueden extraerse indicios de criminalidad en relación a los hechos que denuncia, siquiera sea para corroborarlos periféricamente o que quien los aporte sea el imputado, a los efectos de apoyar su versión exculpatoria de los hechos.

Y la realidad nos indica que un elevado número de denuncias que se interponen por delitos relacionados con la violencia de género o por quebrantamiento de las medidas o penas accesorias de prohibición de comunicación se tramitan como Diligencias Urgentes, que en la mayoría de los casos, se instruyen casi en unidad de acto hasta el señalamiento del juicio oral, por lo que si en el marco de alguno de estos procedimientos que no terminara por sentencia de conformidad se aportaran por alguno de los intervinientes conversaciones de WhatsApp y éstas fueran impugnadas por la otra parte, resultaría de suma complejidad la práctica de la prueba pericial a la que se refiere el Tribunal Supremo en la Sentencia citada, dadas las peculiaridades del marco procedimental al que nos referimos.

Así las cosas, a lo largo de las siguientes páginas nos proponemos analizar las particularidades de esta aplicación de mensajería instantánea, sus posibilidades de alteración o manipulación, los modos en los que puede validarse su acceso al proceso penal, con especial referencia a la prueba pericial y las consecuencias de la impugnación de este medio probatorio por alguna de las partes, para finalmente determinar qué fuerza probatoria puede llegar a otorgársele este medio de prueba y en qué condiciones.

2. Las comunicaciones generadas a través de WhatsApp como medio de prueba en el proceso penal

La oportunidad de incorporar archivos de esta naturaleza al proceso requiere analizar qué medio de prueba será el idóneo para ello. Nuestra decimonónica Ley de Enjuiciamiento Criminal no contempla especialmente estos medios de prueba y el art. 230 de la LOPJ se refiere a los programas y aplicaciones informáticas dirigidas a desarrollar la actividad jurisdiccional, y más concretamente a la documentación de las actuaciones judiciales pero no a los medios de prueba plasmados en soportes telemáticos. No obstante, no existe obstáculo para acudir a una norma más reciente que es de aplicación subsidiaria, como es la Ley de Enjuiciamiento Civil. Así, el art. 299.1 regula los medios de prueba clásicos de los que pueden valerse las partes. Y desde esta perspectiva ha de decirse que los archivos de texto, audio, fotografía o vídeo contenidos en la aplicación WhatsApp de un teléfono móvil como fuente probatoria, podrán tener acceso al proceso como prueba documental (pública o privada, según sea el caso), como prueba pericial, a través del reconocimiento judicial o inspección personal del juez o a través de la prueba de instrumentos tecnológicos del art. 299.2 de la LEC e incluso como prueba personal, a través del interrogatorio del acusado o los testigos, incluida la víctima. Igualmente, el art. 299.3, también referido a los medios de prueba, alude a “cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba adoptando las medidas que en cada caso resulten necesarias”, de lo que se deduce que la LEC establece un *numerus apertus* en relación a los medios de prueba.

Pero además, los datos obtenidos de estas fuentes de prueba han de ser aportados al proceso durante la fase de instrucción en un soporte determinado que pueda ser reproducido en el juicio oral, como puede

ser el papel, resultándole de aplicación en este caso lo dispuesto en los artículos 382 a 384 de la LEC para la prueba documental.

El instrumento probatorio deberá llevarse ante el Secretario Judicial y en la práctica de la prueba registrará el principio de inmediación (art. 289.2 y 3 en relación con el art. 137.1 y 3 de la LEC), bajo sanción de nulidad de pleno derecho. La documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Secretario Judicial, que adoptará también las medidas de custodia que sean necesarias (art. 384.2 LEC). Además, ha de añadirse, que parece lógico y aconsejable que esta diligencia de cotejo se realice inmediatamente después de la incoación de las diligencias urgentes, para que la misma se encuentre disponible en el momento en el que se reciba declaración a la denunciante y al imputado, pues determinados aspectos de la declaración podrían referirse al contenido de esos mensajes instantáneos.

No faltan autores[1] que ponen de manifiesto que además de la presentación en soporte papel del documento que ha de ser objeto de prueba, es conveniente que el Juez que instruye el proceso penal evite ser reacio a la incorporación al proceso de los soportes originales en los que se ha materializado la prueba, acudiendo al recurso de diligenciar las pruebas utilizando la transcripción a los autos a través de la fe pública del Secretario Judicial, ya que ello priva a dicha prueba de matices necesarios que solo puede ser apreciados mediante la reproducción fiel de la misma a través del instrumento en el que aparece recogida, como ocurriría en la grabación de video donde no sólo las imágenes sino también el tono de las palabras ayudarían a determinar, por ejemplo, la seriedad y gravedad de una amenaza proferida.

En cualquier caso, podemos afirmar que el concepto de documento ha cambiado considerablemente, habiéndose introducido en nuestro ordenamiento jurídico una nueva extensión del término como es la de documento electrónico, que según se desprende de lo dispuesto en el art. 3.5 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, será la información de cualquier naturaleza en forma electrónica archivada en un soporte electrónico según formato determinado y susceptible de identificación y tratamiento diferenciado.

La STS nº 1066/2009, de 4 de noviembre de la Sala II, establece que la prueba contenida en soportes telemáticos u obtenida a través de ellos, gozará de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales. A estos dos conceptos se refiere también art. 382.2 de la LEC. Por autenticidad ha de entenderse la propiedad o característica que garantiza la certeza y realidad de los datos por los caracteres que en el mismo concurren, mientras que la integridad ha de hacer referencia a la inalterabilidad de los datos de forma no autorizada.

3. Particularidades del funcionamiento de la aplicación WhatsApp y las posibilidades de manipulación de la misma

Las aplicaciones de mensajería instantánea como WhatsApp, Line o Telegram instalables en teléfonos móviles o en algunas tablets, tienen la particularidad de establecer comunicaciones bidireccionales o multidireccionales entre usuarios mediante las cuales se envían y reciben mensajes de texto, fotografías, notas de audio o vídeos. A través de ellas, también pueden compartirse contactos y la propia ubicación. Se rigen por reglas completamente distintas a las los blogs o a las redes sociales en las que la información que se aporta a aquellos queda almacenada, al menos por un tiempo, en las bases

de datos del administrador.

La principal peculiaridad de la aplicación WhatsApp y lo que a la vez constituye un gran obstáculo para verificar su autenticidad e integridad en el marco de un procedimiento judicial, es que la información transmitida no es conservada en un servidor externo perteneciente al administrador y sólo se conserva en el dispositivo de quienes se comunican, de forma que si todos o alguno de los comunicantes borra total o parcialmente el contenido de una conversación, la misma desaparece del terminal desde el que se procede al borrado, quedando almacenados en segundo plano en la memoria flash donde se mantiene hasta el momento en que la necesidad de espacio en la memoria implica su eliminación, pues se solapan unos datos encima de otros. De lo anterior resulta que la única forma de acreditar la existencia de estos contenidos es a través de los teléfonos móviles que han intervenido como emisor y receptor. No se guardan, pues, en la tarjeta SIM, sino en memoria interna del aparato o en la tarjeta de memoria tipo SD, la cual, si es trasladada a otro terminal no puede recuperar la información que haya sido borrada intencionadamente por el usuario.

Así pues, el administrador de la aplicación, se limita a hacer posible el tránsito de la información entre los comunicantes, utilizando protocolos de seguridad para garantizar el cifrado de esa información. La única información que pueden facilitar es la que se denomina metadatos, que pueden ser definidos como datos sobre datos o la información generada por los usuarios cuando utilizan tecnologías digitales[2]. Tienen la consideración de metadatos, la constatación del tráfico de las comunicaciones, origen y destino de las mismas, datos conservados sobre identidades y nombres de usuario y claves, incluidos el número de abonado telefónico asociado o la IP de referencia. No obstante, todos los datos de tráfico de esta aplicación, incluidas las conversaciones futuras, pueden ser objeto de interceptación a través de la correspondiente autorización judicial, pero el acceso a contenidos ya emitidos no resulta posible si se acude al administrador de la aplicación.

La consecuencia que puede extraerse de lo que se acaba de exponer es que en el caso de la mensajería instantánea, por una parte, pueden borrarse los mensajes total o parcialmente modificando el contexto de la conversación y por otra, que existen mecanismos que permiten crear ex novo mensajes de texto, editar los recibidos o simular el envío y recepción, manipulando incluso su hora.

La Asociación de Internautas publicó en agosto de 2014[3] en su página web un informe en el que documenta los distintos modos de crear y modificar mensajes recibidos de WhatsApp sin la necesidad de tener grandes conocimientos técnicos.

También se situaría en un nivel básico de intrusión la manipulación de una red local wi-fi. Y en un nivel que requiere mayores conocimientos técnicos podría mencionarse el copiado o clonado de la Mac Address o dirección Mac que es un identificador único para cada dispositivo de red y sirve, por ejemplo, para que nuestro router asigne una IP estática a nuestro aparato o para identificar a un usuario dentro de una red informática, así como para geoposicionar personas y de esta forma espiar hábitos y movimientos con una precisión mucho más alta que una dirección IP. A través de la manipulación de la Mac Address con un método conocido como Mac spoofing es posible hacer creer a otras personas o integrantes de la red que nuestra Mac Address es diferente a la real.

Y aún pueden añadirse otros métodos más burdos al alcance de cualquiera como asignar un nombre de usuario a la persona que se quiere dañar, simular el envío de mensajes y a partir de allí aportar al

proceso un documento impreso con la captura de pantalla que contenga el mensaje o archivo correspondiente, alegando la pérdida, borrado o destrucción del mensaje o incluso del propio terminal telefónico.

Así las cosas, pueden comprobarse que las vulnerabilidades del sistema son numerosas y que pueden ser utilizadas para causar algún mal a las personas, por lo que de entrada ha de afirmarse que será difícil que el soporte en el que se contiene la prueba permita considerar que nos hallamos ante una prueba fehaciente, ya que salvo en el caso de pericial de expertos informáticos, en el resto de supuestos ni la fe del Secretario Judicial podría acreditar que se ha producido el hecho sin lugar a dudas[4].

4. El difícil encaje de los postulados de la STS 300/2015 en el marco de las diligencias urgentes

Tras las cuestiones que han sido hasta ahora expuestas, nos proponemos a continuación llevar a cabo un análisis en torno a la práctica de la prueba de los contenidos de WhatsApp en el marco de las diligencias urgentes, y en particular en las que se refieren a delitos relacionados con la violencia de género. Como decíamos ut supra, resulta habitual que el devenir diario de los asuntos que han de tramitarse en un Juzgado de Violencia sobre la Mujer sea voluntad de alguna de las partes el querer aportar al procedimiento algún contenido de la aplicación de mensajería WhatsApp para reforzar su respectiva versión de los hechos mantenida en el procedimiento. No son pocas las ocasiones en las que se puede ver cómo el agresor ha remitido a la víctima mensajes escritos o de voz cuyo contenido podría ser constitutivo de delito. Y también el agresor en muchas ocasiones tiene interés en realizar alguna aportación de estas características.

El art. 87 ter de la LECrim. otorga a los Juzgados de Violencia sobre la Mujer competencia para conocer de determinados delitos, los cuales y según expresa el art. 795 del mismo texto legal, si se trata de delitos de lesiones, coacciones, amenazas o violencia física o psíquica habitual, cometidos contra las personas a que se refiere el art. 173.2 del Código Penal y por tanto contra quien sea o haya sido su esposa, o mujer que esté o haya estado ligada al autor por análoga relación de afectividad, aun sin convivencia, podrán tramitarse como diligencias urgentes, dado que llevan aparejada una pena privativa de libertad que no excede de 5 años u otras penas, bien sean únicas, conjuntas o alternativas, cuya duración no excede de diez años, pues este es el ámbito objetivo del procedimiento del que tratamos, siempre que además, reúnan las restantes condiciones a las que se refiere el precepto (se inicien por atestado policial, se cite a las personas ante el Juzgado y se trata de hechos de sencilla instrucción).

Además la LO 7/2015 de 21 de julio, de reforma de la LOPJ, ha añadido al art. 87 ter el apartado g), de forma que a partir del 1 de octubre de 2015, los Juzgados de Violencia sobre la Mujer serán también competentes para conocer de la instrucción de los procesos para exigir responsabilidad penal por el delito de quebrantamiento previsto y penado en el art. 468 del Código Penal, cuando la persona ofendida por el delito cuya condena, medida cautelar o medida de seguridad se haya quebrantado sea o haya sido su esposa, o mujer que esté o haya estado ligada al autor por una análoga relación de afectividad aun sin convivencia. Y se da la circunstancia que en este tipo de delito el contenido de las comunicaciones realizadas mediante esta aplicación de mensajería instantánea pueden constituirse como un medio de prueba de gran trascendencia, hasta el punto de que en ocasiones llegarán a ser el medio a través de la cual se ha cometido el delito, como ocurriría en los casos de quebrantamiento de las prohibiciones de comunicación que hubieran sido acordadas en otro procedimiento como medida de protección hacia la víctima.

Según la Memoria de 2015[5] de la Fiscalía General del Estado, en el año 2014 se incoaron 47.331 diligencias urgentes en los Juzgados de Violencia sobre la Mujer de todo el territorio español, de las cuales 11.054 se elevaron al Juzgado de lo Penal para la celebración de juicio oral. En cuanto a las restantes, o bien se alcanzó una conformidad o bien se transformaron en diligencias previas o se sobreseyeron.

Desde el punto de vista legal y en lo que afecta a la instrucción de las diligencias urgentes no existe ninguna limitación legal en cuanto al contenido material de las diligencias de instrucción que pueden practicarse. En este sentido deberán practicarse aquellas que la instrucción de la causa requiera, igual que si se tratara de unas diligencias previas o de un sumario ordinario. Pero no puede negarse que existe una limitación de carácter procesal o temporal pues las diligencias urgentes están concebidas para ser terminadas prácticamente en unidad de acto. Tras oír a denunciante e imputado, en ocasiones llega a practicarse alguna declaración testifical, se une el informe Médico Forense si hubiese algún resultado lesivo, la hoja histórico penal, la tasación de daños, si los hubiere, así como alguna otra prueba documental si resulta necesario, como sería el supuesto de los delitos de quebrantamiento en el que habrá de unirse a las actuaciones los testimonios de la resolución judicial dictada en el marco de otro procedimiento en la que se acordaran medidas cautelares o penas accesorias para la protección de la víctima, así como las notificaciones a las partes y el requerimiento efectuado al imputado en relación a las consecuencias que eventualmente podrían derivarse en caso de incumplimiento de esas medidas o penas accesorias. Verificado lo anterior, la LECrim. en el art. 798, ordena al Juez oír a las partes sobre la resolución que ha de dictarse y en este momento, el instructor deberá adoptar una resolución en el que declare las diligencias practicadas suficientes o insuficientes en una resolución contra la que no cabe recurso alguno.

En el supuesto de que se declararan insuficientes, se producirá la transformación a diligencias previas. Y si las declara suficientes deberá dictar en forma oral auto de preparación del juicio oral, tras el cual, las acusaciones se pronunciarán sobre si procede o no la apertura del juicio oral, siendo que en caso positivo deberá presentarse por el Fiscal escrito de acusación en el mismo momento, concediendo el texto legal un plazo a la acusación particular a los mismos efectos. Como es sabido, la celeridad en la instrucción es lo que preside la tramitación de las diligencias urgentes.

El problema surge cuando las acusaciones o la defensa solicitan la práctica de diligencias de instrucción que no pueden realizarse de forma inmediata. Y aquí retomamos nuevamente la cuestión relacionada con la controversia que puede surgir en torno a la aportación al proceso de la fuente de prueba extraída de la aplicación de mensajería instantánea.

Generalmente, como hemos apuntado esta fuente de prueba accederá al proceso a través de la prueba documental y más concretamente a través del cotejo por parte del Secretario Judicial del contenido de las conversaciones, archivos de audio, vídeo o fotografías que pretendan hacerse valer como prueba por alguna de las partes. La tarea resulta costosa y prolija, sobre todo si se trata de un número elevado de conversaciones, pues se hace necesaria su transcripción a soporte papel y posterior cotejo. Podría también ser aportada por la parte que pretende hacerla valer, lo que evitaría la fase de transcripción, o incluso ser remitido el contenido de un concreto chat desde el teléfono móvil a una dirección de correo electrónico, pasándose directamente a la fase de cotejo.

Pero como ya hemos puesto de manifiesto, esta aplicación de mensajería instantánea puede ser objeto de fácil manipulación. Y llegados a este punto es cuando surge la compleja cuestión relacionada con una eventual impugnación de esta prueba documental por alguna de las partes, incluido el Ministerio Fiscal.

Ninguna trascendencia tendría, a nuestro juicio, que en este momento se impugnara el contenido de esta prueba negándole valor probatorio, pues este hecho forma parte de la facultad que de valorar la misma tiene el Juez que haya de dictar sentencia. Pero cuestión distinta es que la impugnación se refiera a la autenticidad o integridad de la prueba.

Como apuntábamos al inicio, la reciente STS 300/2015, de 19 de mayo, Ponente Manuel Marchena Gómez, abre una corriente doctrinal en relación a las cautelas que han de tenerse respecto de este tipo de pruebas. En ella y en relación a una acusación de abusos sexuales, la defensa había impugnado la autenticidad de unas conversaciones mantenidas en una red social entre la víctima y un tercero y en relación a las conversaciones realizadas a través de un medio electrónico, se expresa en los siguientes términos:

“Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido”.

Como dice la doctrina[6], la sentencia nos sitúa ante varios retos: el primero de ellos es reconocer la vulnerabilidad, fragilidad, de este medio de prueba, en el sentido de ser fácil objeto de manipulación o falseamiento. En segundo lugar, el establecimiento de una carga probatoria en quien aporta una prueba electrónica en soporte impreso, si la misma es objeto de impugnación y por último, la preferencia por la necesaria práctica de una prueba pericial que pueda dar luz sobre la identidad de los interlocutores y la autenticidad-integridad de los contenidos.

Pero de todas las perspectivas que se apuntan en la sentencia, ha de considerarse que la que más interesa en este momento en relación al asunto que nos ocupa, es la que hace referencia a la imposición de una regla de carga probatoria que ha de recaer en quien aporta dicha prueba documental al juicio, correspondiéndole acreditar el verdadero origen de esa comunicación, la identidad de los interlocutores y la integridad de su contenido. Esta carga probatoria podrá recaer tanto en las acusaciones como en la defensa.

5. La impugnación de la prueba documental

5.1. Sobre el momento procesal oportuno para realizarla

Se entiende, en general, por impugnación el cuestionamiento de la validez de esta prueba, no estando previsto especialmente este mecanismo para la prueba electrónica, sino tan sólo en la normativa

general[7].

En lo que afecta a la impugnación de la autenticidad e integridad, la prueba documental consistente en los contenidos extraídos de la aplicación de mensajería instantánea aportados por alguna de las partes, debemos distinguir dos aspectos: el momento en que deberá hacerse efectiva esta impugnación y los argumentos o motivos en los que se basa la misma.

En cuanto al momento en que ha de realizarse la impugnación, situados en el marco de la fase de instrucción de las diligencias urgentes, entiendo que puede sentarse un criterio general en base al cual, la impugnación ha de hacerse tan pronto como la parte a quien perjudique tenga conocimiento de la misma. Pero además de este criterio general, podríamos hablar de tres momentos procesales que se presentan como idóneos para ello, como son: durante la instrucción, en el momento de presentar escrito de conclusiones provisionales o de defensa y en el inicio de la vista oral.

Así pues, tras la diligencia de cotejo de los documentos consistentes en contenidos de mensajería instantánea presentados por una de las partes, deberá realizarse el traslado a las restantes partes, incluido el Ministerio Fiscal. Como se ha expuesto con anterioridad ha de remarcarse la conveniencia de que la diligencia de cotejo se realice lo antes posible, incluso antes de las declaraciones de las partes, lo que no suele ocurrir en la práctica por regla general, si bien contar con la diligencia de cotejo en el momento de practicar las declaraciones de las partes resultaría muy útil, pues podría preguntárseles sobre su contenido. En el momento en que los intervinientes dispongan del mismo, la parte o partes que no hayan presentado el documento o documentos, deberán analizar su contenido para estudiar la oportunidad de una eventual impugnación.

Si el eventual impugnante es el imputado, ningún problema ha de existir, ya que necesariamente estará representado por Letrado. Pero debería también contemplarse otro supuesto, que fácilmente puede darse en la práctica, que se refiere a que la aportación de documentos susceptibles de ser impugnados la haya realizado el imputado y fuera el caso de que la víctima no tuviera representación legal, por haber declinado la posibilidad de constituirse como acusación particular. En este supuesto, parece claro que debería el Ministerio Fiscal reunirse con la víctima para analizar el contenido del documento resultante del cotejo, para conocer la opinión de la víctima sobre la autenticidad e integridad de los contenidos aportados y su correspondencia con la realidad, ya que en caso de ser necesaria la impugnación sería el Ministerio Fiscal quien debería realizarla.

No obstante, en este momento procesal, al Juez de Instrucción no se le ha de exigir pronunciamiento alguno en torno a esas impugnaciones, pues no le corresponde, ya que se trata de una decisión que deberá adoptar el órgano enjuiciador.

Pero alertada una de las partes o el Ministerio Fiscal de la impugnación realizada, sería este el momento idóneo para proponer al Juez de Instrucción la práctica de una prueba pericial, si bien, habría de proponerla como diligencia de instrucción. Y si la práctica de la prueba pericial fuera acordada por considerar, en el trámite del art. 798.2,1º, que las diligencias son insuficientes, sería necesaria la transformación del procedimiento a diligencias previas para la práctica de la prueba pericial a la que se refiere el Tribunal Supremo en la sentencia que se comenta. Y si en el mismo trámite, la decisión del Juez fuera denegar esa diligencia de instrucción por considerar las diligencias suficientes, la parte a quien perjudicara la decisión de no practicar la prueba pericial electrónica, no podría interponer recurso

contra esa resolución, pues así lo dispone el precepto citado y se vería abocada a proponer la prueba nuevamente en el escrito de conclusiones provisionales como prueba pericial anticipada, al amparo de lo dispuesto en el art. 657.3 de la LECrim., el cual al regular los escritos de conclusiones provisionales faculta a las partes para pedir que se practiquen desde ese momento aquellas diligencias de prueba que por cualquier causa se tenga temor de que no se vayan a poder practicar en el Juicio Oral, o que pudieran motivar su suspensión. Y en este último caso, la solución se presenta como distinta atendiendo a quien sea la parte que realice tal impugnación. Si son las acusaciones o alguna de ellas, incluido el Ministerio Fiscal quienes quieren hacer valer la prueba y han de defenderse de la impugnación que de la misma se ha realizado en fase de instrucción, habida cuenta de la denegación por el instructor de la prueba pericial, podrán proponer su práctica en el escrito de conclusiones provisionales. Pero si es la defensa quien en el escrito de defensa formaliza la impugnación de la autenticidad e integridad de la prueba documental que había sido aportada por la acusación, al no encontrarse prevista tras el escrito de defensa la posibilidad de conceder un nuevo traslado a la acusación, el momento procesal hábil para que la acusación o acusaciones propongan la práctica de la prueba pericial electrónica sería el inicio del juicio oral, a través del planteamiento de una cuestión previa, al amparo de lo previsto en el art. 786.2 de la LECrim., siendo este el tercero de los momentos procesales apto para proponer la prueba pericial a la que nos estamos refiriendo.

Pero si el que acuerda su práctica es el órgano de enjuiciamiento en el momento en que recibe en procedimiento que es cuando le corresponde examinar la pertinencia de la totalidad de las pruebas propuestas, por lo general y en aquellos Juzgados de lo Penal que por el volumen de trabajo cumplen los plazos de señalamiento legalmente establecido, no podría mantenerse el señalamiento del juicio rápido que se habría hecho en el Juzgado de Violencia sobre la Mujer, por imposibilidad material de tener realizada la prueba pericial en el plazo de 15 días que marca el art. 800.3 de la LECrim.

5.2. Sobre los motivos de la impugnación

Se ha referido con anterioridad que si la impugnación se refiere al hecho de no otorgarle a la parte impugnante el mismo valor probatorio que quien la ha presentado, esta alegación no tiene trascendencia alguna a los efectos de la práctica o no de una prueba pericial, ya que se refiere al contenido mismo de la prueba y no a su autenticidad o integridad. Pero avanzando en el asunto que nos ocupa, ha de analizarse si cualquier tipo de impugnación de la parte a quien perjudique el contenido de la prueba documental de contenidos de mensajería ha de ser suficiente para que la parte contraria solicite la práctica de la prueba pericial. ¿Servirá cualquier impugnación? O ¿deberán exponerse de forma exhaustiva los motivos por los que se realiza, aportando incluso un principio de prueba o indicio que apoye esas manifestaciones?

La respuesta es clara. No cualquier impugnación será suficiente. Las alegaciones que duden de las condiciones de autenticidad o de exactitud de la prueba en las que se fundamente la impugnación han de ser serias, claras y exhaustivas, es decir, han de tener la suficiente entidad para que se produzca el efecto del desplazamiento de la carga de la prueba y la misma recaiga en la parte que aportó al proceso esos documentos impugnados, quien deberá entonces proponer la prueba pericial.

Para apreciar si existe una impugnación con suficiente seriedad, podrán tenerse en cuenta varios elementos[8]:

– En primer lugar, la existencia de razones en las que se fundamente la concreta impugnación, así como

el propio contenido de las mencionadas razones, porque en la práctica hay ocasiones en que concurre una mera manifestación impugnatoria sin respaldo alegatorio.

– En segundo lugar, la propia diligencia de la parte impugnante al proponer medios probatorios que puedan menoscabar la integridad y/o autenticidad de la prueba digital propuesta de contrario, que ha de ser apreciada en relación con la postura procesal de la parte que propuso la prueba digital. En este sentido, la STS 300/2015, de 19 de mayo, otorga eficacia probatoria a la prueba basándose en dos razones, siendo una de ellas "el hecho de que fuera la propia víctima la que pusiera a disposición del Juez de instrucción su contraseña del mensaje con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial"; y la STS recoge posteriormente la alusión de la sentencia de la Audiencia Provincial en el sentido de que la defensa no hizo ninguna petición al respecto.

En este sentido, la SAP de Vizcaya de 24 de julio de 2014, aunque referida a un delito de receptación, ante una impugnación de la prueba documental dice lo siguiente:

“la mera protesta de que el WhatsApp es manipulable y de que las conversaciones pudieron ser mantenidas por el anterior titular, es manifiestamente insuficiente para alterar la valoración probatoria en el sentido interesado en el recurso. Todo apunta a la autoría de la receptación por el acusado, ya que los objetos sus traídos aparecen en su teléfono que él dice adquirido de segunda mano, sin dar ningún dato sobre a quién, persona desconocida que además habría resultado ser el autor de los mensajes de WhatsApp. En opinión del Tribunal, esta versión no tiene el relieve necesario ni la credibilidad mínima para representar una hipótesis alternativa razonable a la que la sentencia ha elevado a categoría de hechos probados en la sentencia sobre la base de la prueba practicada en el juicio oral”.

6. La prueba pericial electrónica o informática en el marco de las diligencias urgentes

Llegados a este punto, abandonamos la cuestión relacionada a la impugnación de la prueba para situarnos ante un eventual momento en el que se ha de llevar a cabo su práctica, pues ello es lo que recomienda la STS 300/2015, de 19 de mayo cuando indica que en todos estos supuestos, la cautela con la que han de mirarse estas pruebas, dada la facilidad de su manipulación aconseja que impugnada la prueba documental, ha de practicarse una prueba pericial.

Y así las cosas, considero que tres son las cuestiones de calado a las que deberemos enfrentarnos en el supuesto de que sea necesaria la práctica de una prueba pericial de esta naturaleza.

La primera, guarda relación con las características particulares de las aplicaciones de mensajería instantánea, que como ya hemos comentado, a diferencia de lo que ocurre con Facebook, Twitter u otras aplicaciones, en el caso de WhatsApp el administrador de la aplicación no guarda en sus archivos el contenido de estas conversaciones, por lo que la posibilidad de practicar una prueba pericial queda notablemente limitada, al no poder contar con una copia auténtica e indubitada del contenido de las comunicaciones originales.

La segunda, se refiere al concreto marco procedimental en el que nos encontramos como son las diligencias urgentes, las cuales por sus propias características nacieron para tramitarse con celeridad y en unidad de acto, lo que se presenta como opuesto a la oportunidad de practicar una prueba pericial de estas características, en un espacio temporal que sea compatible con la rápida instrucción de la causa.

La tercera de las cuestiones tiene que ver con la superación de unos límites relacionados con los derechos fundamentales de las personas, como son el derecho al secreto a las comunicaciones, la protección de datos de carácter personal y el derecho a la intimidad, pues a través de la prueba se tratará de analizar el contenido de la información que obra dentro del terminal telefónico, por lo que se requerirá el consentimiento de las partes o en su caso, autorización judicial.

En relación al consentimiento, hemos de plantearnos el supuesto de la negativa de las partes o de alguna de ellas en el caso de que fuera necesario que el perito informático analizara el contenido de los terminales telefónicos de ambas partes. Parece a priori que no resulta lógico que no preste su consentimiento la parte que ha aportado la información a través de la prueba documental. Y tampoco, parece razonable que no preste su consentimiento quien ha realizado la impugnación de la prueba, aunque esta negativa tanto en uno como otro caso podría tenerse en cuenta en el momento de la valoración de la prueba. Pero que no resulte lógico ni razonable no quiere decir que no resulte posible, por lo que ante la falta de consentimiento para acceder al terminal telefónico hemos de plantearnos si resulta posible suplirlo a través de una autorización judicial.

El art. 5 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, parece limitar el acceso a dichos datos cuando nos encontremos ante delitos graves. Y si delito grave es el que lleva aparejada una pena grave, en lo que se refiere a los delitos relacionados con la violencia de género que pueden tramitarse en el marco de las diligencias urgentes, los mismos están castigados todos ellos con penas menos graves o leves, por lo que inicialmente parece que no sería posible en estos casos hacer uso de los datos conservados por los administradores del servicio de mensajería. Ciertamente, el acceso a datos almacenados en dispositivos telefónicos puede conllevar el análisis de una cantidad elevada de información que los mismos se almacenan con una posible afectación de derechos fundamentales, por lo que inicialmente habrá de mantenerse que habrá de realizarse un juicio de proporcionalidad entre el fin perseguido con la autorización al acceso y el grado de afectación de derechos fundamentales de la persona propietaria del terminal, que puede ser tanto la víctima como el imputado o incluso un tercero con el que se hubieran comunicado alguno de los anteriores. Así las cosas, parece que inicialmente estaríamos cerrando la posibilidad de realizar esta prueba en el caso de delitos leves y de los delitos menos graves como son los de la violencia de género. Pero a mi juicio, el recurso a la gravedad del delito no habría de convertirse en un obstáculo en este caso, pues la redacción de la Ley 25/2007 se refiere a un momento en el mundo de la telefonía móvil se encontraba mucho menos evolucionado. Apenas existían las redes sociales y no había sido creada la aplicación WhatsApp, la cual fue ideada en 2009. Además, no puede olvidarse que en la lucha contra la lacra que representa la violencia de género deben encontrarse mecanismos capaces de otorgar una eficaz protección a la mujer que es víctima de esta violencia machista. Un informe de la comisión de Desarrollo Digital de la ONU presentado en septiembre de 2015 pone de manifiesto que un 73% de la población femenina de todo el mundo que utiliza Internet ha experimentado o ha estado expuesta a alguna forma de violencia. La ciberviolencia incluye, entre otros delitos, el discurso del odio, la interceptación de mensajes privados, el acoso criminal, sexual o las amenazas.

Y así las cosas, de la misma manera que en el art. 503.3 c) de la LECrim. se establece que no ha de atenderse a límite cuantitativo alguno de sanción punitiva para acordar la prisión provisional si la finalidad es proteger a la víctima, parece que podría aplicarse algún criterio similar en este supuesto,

pues si en el anterior argumento se encuentra justificación para llevar a cabo una injerencia en el derecho fundamental a la libertad, parece que realizar esa injerencia en otros derechos fundamentales como el de la intimidad o el secreto de las comunicaciones se presenta como una invasión de menor envergadura.

Un ejemplo de ello lo encontramos en la SAP de 27 de febrero de 2015 dictada por la Sección Cuarta de la Audiencia Provincial de Madrid dictada en un procedimiento en el que se perseguían delitos de calumnias e injurias cometidas a través de Internet y en el que se había rechazado por el Juzgado de Instrucción acudir a la investigación tecnológica para averiguar la identidad del querellado por no encontrarnos ante un delito grave. La Audiencia Provincial pone de manifiesto que estas conductas pueden generalizarse si se instala en la sociedad una sensación de impunidad por el hecho de haberse establecido trabas legales o judiciales en el esclarecimiento de los hechos, dejándose desprotegidos determinados bienes jurídicos por el hecho de haber sido vulnerados a través de redes públicas de comunicaciones. Por ello, todas estas circunstancias permiten valorar como socialmente graves estos hechos delictivos.

Así pues, si se acepta como posible el argumento de que aún en caso de falta de consentimiento de titular del teléfono resulta posible autorizar judicialmente el practicar una prueba pericial informática, deberá analizarse la memoria de los correspondientes terminales, a ser posible supuestos emisor y receptor, pues son los que pueden aportar razón sobre la realidad de emisión de un mensaje por determinado terminal y si el mismo ha sido objeto de algún tipo de manipulación. Y ello, deberá realizarse lo antes posible, pues en estos casos cuanto más tiempo haya transcurrido entre el registro de un dato hasta su búsqueda, menores son las posibilidades de recuperación de esos datos. Y además, la clave para conseguir el máximo nivel de fiabilidad en un examen pericial dirigido a la constatación de la realidad, origen y no sometimiento a manipulación de un determinado mensaje de mensajería instantánea o comunicación cursada a través de plataforma de redes sociales, pasa por la disponibilidad de las fuentes y soportes originales[9].

En el supuesto en que se hayan empleado programas espía u otras modalidades de software malicioso que permitirán la emisión de mensajes desde el propio terminal usurpado o aprovechando la información obtenida sobre clave de seguridad, nombre de usuario y clave de acceso, etc., la solución parte de un examen exhaustivo de la memoria interna del terminal.

La investigación pericial se centrará en verificar en el volcado de la memoria, de los códigos propios de estos programas; localizar la dirección IP del servidor al que reenvía los datos en su caso; localizar el número de abonado teléfono oculto con el que se conecta para reenviarle la información, y en los archivos temporales localizar la datación de la instalación del programa.

No obstante lo anterior, también se ha puesto en duda el nivel de fiabilidad de este tipo de pericial concediéndoles un carácter limitado y no absolutamente incontestable, lo cual se presenta como obstáculo para su aceptación. Este carácter incontestable dependerá de muchos factores, como si puede accederse o no a la fuente original, dado que el administrador del servicio no puede aportar ninguna información sobre contenidos, y de si se puede disponer de la información de emisor y receptor y también del grado de cualificación del perito, así como de su experiencia profesional y de las herramientas a su disposición, careciendo de interés, a efectos probatorios, aquella pericial que se limite a indicar que una determinada conversación se encontraba almacenada en la base de datos de

mensajería de un determinado terminal. Es imprescindible que se descarte de algún modo la existencia de manipulación, para lo cual, se precisará un perito con alto grado de cualificación profesional, como por ejemplo un experto en seguridad informática, lo que hace suponer que la pericia tendrá un coste elevado que en muchos casos será desproporcionado con el resultado que se pretenda obtener de ella.

7. Consideraciones finales

Así las cosas y ante este escenario, parece que la práctica de un prueba pericial informática sobre contenidos enviados o recibidos a través de la aplicación WhatsApp, por los numerosos motivos apuntados, se asemeja a una carrera de obstáculos que no siempre podrán ser superados con éxito. Obstáculos algunos de ellos derivados de las propias características de la aplicación de mensajería, en la que no puede descartarse una manipulación de los mensajes aportados o el hecho de que el administrador de la aplicación no conserve el contenido de las conversaciones o archivos de vídeo, audio o fotografías, lo que implica la posibilidad de que no pueda contarse con archivos originales en el caso de que una de las partes haya borrado la información y no pueda esta ser recuperada de la memoria flash, ya que cuando ésta se llena las nuevas informaciones se solapan encima de las anteriormente guardadas. Otros de carácter procesal, que residen en el hecho de que el desarrollo de la prueba necesariamente se prolongará más allá del corto lapso temporal en el que se tramitan unas diligencias urgentes, dado que pueden contarse hasta tres momentos procesales que serían aptos para la proposición de la prueba pericial que la STS que se analiza considera necesaria tras la impugnación de la prueba documental. Otros con raigambre en el derecho material y los derechos fundamentales, que cuestionan el hecho de que ante la falta de consentimiento de los titulares del teléfono, pudiera concederse una autorización judicial que justificara la injerencia en derechos fundamentales tales como la intimidad, el secreto de las comunicaciones o la protección de datos, pues la realización de la prueba pericial requeriría de un análisis exhaustivo del contenido del teléfono o teléfonos, siendo necesario analizar tanto datos relacionados con el delito que se investiga como otros datos ajenos al mismo.

Quizás por lo anterior, la STS 300/2015 no habla estrictamente de preferencia sobre esta prueba pericial sino del carácter indispensable de su práctica en caso de impugnación para identificar el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Por ello, la propia sentencia matiza más tarde esta afirmación apuntando la posibilidad de contradecirla a través de otros medios probatorios en el caso de que no sea posible la práctica de la prueba pericial, tales como las declaraciones en el plenario de los comunicantes, el ofrecimiento de los mismos de sus terminales telefónicos para que se proceda al examen del contenido y la posición de la defensa en torno a todas estas circunstancias, pareciendo expresar así que no puede ser aceptada cualquier impugnación sino sólo aquella de verdadera entidad, pues en el caso de que no la alcance la prueba documental electrónica pasará a formar parte del acervo probatorio para su libre valoración por el Juez junto las restantes pruebas que se hayan practicado.

[1] Pérez Astudillo, N., “Los medios telemáticos como prueba de cargo en el proceso”, Cuadernos Digitales de Formación nº 3, 2015, Consejo General del Poder Judicial, pág. 14.

[2] Pérez Astudillo, N., “Los medios telemáticos como prueba de cargo en el proceso”, Cuadernos Digitales de Formación nº 3, 2015, Consejo General del Poder Judicial, pág. 8.

[3] <http://www.internautas.org/html/8474.html>

[4] Pérez Astudillo, N., “Los medios telemáticos como prueba de cargo en el proceso”, Cuadernos Digitales de Formación nº 3, 2015, Consejo General del Poder Judicial pág. 6.

[5] https://www.fiscal.es/fiscal/publico/ciudadano/documentos/memorias_fiscalia_general_estado

[6] Rodríguez Lainz, J.L., “Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea”, Diario La Ley, nº 8569, Sección Doctrina, 25 de junio de 2015, pág. 34.

[7] Mariscal de Gante y Mirón, R. M., “Email, sms y WhatsApp: nuevos “modos” de prueba documental”, SP/DOCT/19021, Editorial Jurídica Sepin, abril 2015, pág. 5.

[8] Delgado Martín, J., “La prueba del whatsapp”, Diario La Ley, nº 8605, Sección Tribuna, 15 de septiembre de 2015, -Editorial Le Ley, pág. 9.

[9] Rodríguez Lainz, J.L.,” Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea”, Diario La Ley, nº 8569, Sección Doctrina, 25 de junio de 2015, pág. 13.

<http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533/>