**Dictamen nº 1/2016** ***Sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas***

Con fecha 1 de octubre del pasado año 2015, el Delgado de Criminalidad Informática de la Fiscalía provincial de Badajoz, Ilmo. Sr. Don Julio López Ordiales, elevó consulta a esta Unidad Central del Área de Especialización en la que sometía a nuestra consideración la Nota de Servicio, elaborada por dicho Fiscal Delegado, en la que se fijaban criterios para la valoración de las pruebas documentales relativas a comunicaciones electrónicas presentadas como tales en procesos judiciales en el ámbito penal. En el mismo documento el citado Delegado sugería la oportunidad de difundir el contenido de dicha Nota informativa a los restantes Delegados en el marco de lo establecido en la Instrucción 1/2015 FGE.

En la referida Nota de Servicio, cuya copia se adjunta, se hace referencia a la cada vez más frecuente aportación por las partes en procesos penales, como medio de prueba de cargo o de descargo, de documentos en soporte físico en los que se transcriben conversaciones o contactos canalizados por sistemas de comunicación electrónica o aplicaciones para móvil y que se generan a través de la impresión del texto escrito de la comunicación cursada por correo electrónico o de las capturas de pantalla –el llamado "pantallazo"- de las conversaciones efectuadas por Whatsapp o por cualquier otro sistema de mensajería instantánea, o de aquellos otros que se realizan a través de las plataformas de las redes sociales.

El informe elaborado por el Fiscal Delegado de Badajoz reflexiona acerca de las posibilidades reales de simulación y/o alteración de estas evidencias tanto en lo que se refiere al origen como al propio contenido de las comunicaciones a que dichos documentos se refieren y sugiere unos criterios de actuación en orden a garantizar su autenticidad e integridad y, en consecuencia, su validez como medio de prueba. Nótese que la cuestión que se plantea se refiere básicamente a medios de prueba aportados por las partes, no a evidencias obtenidas como consecuencia de una intervención policial o de actuaciones acordadas en el curso de un proceso penal tales como, por ejemplo, las resultantes del "volcado" de un dispositivo electrónico. Sin embargo, también en estos últimos supuestos pueden generarse dudas acerca de

posibles manipulaciones o alteraciones producidas en origen, con carácter previo a la intervención del dispositivo. Ciertamente, producida la intervención judicial/policial, contamos con pautas claras sobre cadena de custodia para garantizar precisamente el tratamiento de la evidencia y su autenticidad e integridad a partir de esa intervención pero ello no permite descartar que la manipulación se haya producido con anterioridad a dicha intervención a través de actuaciones irregulares sobre los contenidos o sobre el dispositivo mismo investigado.

Es por todos conocido que el desarrollo de las tecnologías de la información y la comunicación, ha puesto a disposición de todos los ciudadanos una diversidad de herramientas aptas para canalizar de forma rápida y eficaz las relaciones entre las personas, las instituciones, los diversos colectivos e incluso los Estados. Como acertadamente recuerda la STS 823/2015 de 24 de febrero *el correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato electrónico, el derecho a la libre comunicación entre dos o más personas.* Muchas de nuestras comunicaciones con los demás se llevan a efecto actualmente a través de estos instrumentos y por tanto de forma electrónica, lo que hace que, en ocasiones, hayamos de recurrir a estas mismas herramientas para poder acreditar determinadas situaciones, el contenido de conversaciones concretas o, en definitiva, los hechos mismos objeto de investigación penal.

Estamos en todo caso ante evidencias fácilmente manipulables que exigen de los operadores jurídicos, y en particular del Ministerio Fiscal, unas especiales cautelas en su valoración como medio de prueba. A ello se ha referido expresamente la Sala Segunda del Tribunal Supremo, en la reciente sentencia 300/2015 de 19 de mayo, a propósito de unos "pantallazos" incorporados a la causa para acreditar una supuesta conversación mantenida entre dos personas a través de *Tuenti.* Según el alto Tribunal *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.* Similar reflexión se ha reiterado en la más reciente sentencia del Alto Tribunal 754/2015 de 27 de noviembre.

Ha de señalarse, no obstante, que aun cuando la literalidad del pronunciamiento parece referirse únicamente a los supuestos de incorporación de los contenidos de las conversaciones electrónicas a través de *archivos de impresión* y no a aquellos en que las partes aportan los archivos electrónicos de que aquellos traen causa, el razonamiento que se efectúa en la sentencia es predicable respecto de ambos supuestos, pues la manipulación puede producirse tanto por alteración de las impresiones como por manipulación del archivo digital, supuesto que será el más habitual y al que se refiere específicamente mencionada sentencia, en cuyo caso la aportación al proceso podrá hacerse bien sea por exhibición del propio archivo o por su aportación, una vez impreso, en soporte físico.

En cualquier caso, ha de entenderse que las consecuencias de la impugnación de la evidencia aportada y, en particular, el desplazamiento de la carga de la prueba a que se refiere la Sentencia, no tiene por qué producirse en todo caso, sino que vendrá determinado necesariamente por la propia razonabilidad y seriedad del planteamiento impugnatorio mismo, cuestión que habrá de valorarse en cada asunto en particular. Ello sin olvidar que, en otros supuestos, de los que es un buen ejemplo el contemplado en la STS 300/2015 antes citada, la impugnación de la evidencia impresa o electrónica devendrá intrascendente al poderse acreditar los hechos y, en particular, la comunicación o contacto cuestionado, por cualquier otro medio probatorio tales como las declaraciones de los intervinientes en el mismo o de terceros que hayan tenido conocimiento de ello, o cuando la propia existencia de la trasmisión o su contenido pueda corroborarse por los restantes elementos de prueba o circunstancias concurrentes

Centrándonos en el análisis de la problemática que nos ocupa y en el establecimiento de criterios de actuación al respecto, resulta conveniente, en primer término, distinguir al menos cuatro diferentes supuestos~~,~~ en atención al sistema o mecanismo de comunicación o traslado de información utilizado, y, en consecuencia, a partir del cual se genera el medio de prueba que se pretende aportar al proceso: a) mensajería instantánea; b) mensajes SMS o MMS; c) correo electrónico y d) comunicación a través de plataformas de redes sociales

En relación con ello, y comenzando por la primera modalidad, ha de tenerse en cuenta que tanto Whatsapp (disponible para terminales móviles con sistema operativo IOS, Blackberry, Android, Symbian y Windows Phone) como los similares sistemas de mensajería instantánea (Line, Telegram….) son aplicaciones que operan por la red móvil o wiffi. Sin perjuicio de ello, Whatsapp actualmente puede también ser usado, visualizado y sincronizado en cualquier PC tras la implementación de la *WhatsApp Web*. Este tipo de aplicaciones de mensajería multiplataforma presentan determinadas notas características que habrán de tenerse en cuenta a estos efectos.

a) Permiten la comunicación entre usuarios pero también el intercambio de fotos, videos e incluso mensajes de voz. Estas transmisiones, en las que la identificación del usuario se realiza a través del teléfono móvil, pueden efectuarse tanto de forma bidireccional como multidireccional, cuando en la comunicación interviene una pluralidad de personas integradas en un grupo de envío.
b) No existe un servidor externo que conserve la información sobre los contenidos de los mensajes sino que la misma se encuentra alojada - generalmente una vez ha sido encriptada- únicamente en las bases de datos alojadas en los propios dispositivos utilizados para llevar a efecto la transmisión o, en su caso, accesibles desde los mismos cuando se haya configurado la aplicación para hacer copias en la nube.

Cuestión diferente es la referida a los mensajes SMS (Short Message Service) o a la mensajería multimedia MMS (Multimedia Messaging Service). Estos sistemas de comunicación se articulan a partir de servicios prestados por los operadores de telefonía móvil para el envío por red privada de mensajes cortos o de contenidos multimedia –incorporando videos o fotos-. En este caso ha de tenerse en cuenta las siguientes características:

a) Están planteados para comunicaciones de carácter bidireccional, en los que únicamente existe un usuario emisor y un usuario receptor, aun cuando el mensaje pueda enviarse simultáneamente a varios destinatarios.
b) Los SMS son procesados en un centro de servicios de mensajes cortos SMSC (Short Message Service Center). En el caso de los MMS el centro de servicios se denomina MMSC (Multimedia Message Service Center) En ambos casos el centro de servicio se encarga de comprobar si el receptor destinatario está operativo, almacenando temporalmente, por el tiempo mínimo imprescindible, el envío hasta que esta circunstancia se produce.

Por su parte, el correo electrónico presenta peculiaridades en relación con los anteriores sistemas de comunicación examinados:

a) Permite el intercambio de mensajes de texto y también de la documentación digital que en su caso le acompañe (imágenes, videos, documentos…). La comunicación puede dirigirse a una sola persona o a una pluralidad de personas simultáneamente que se hacen figurar como destinatarios de un mismo correo o que figuran en copia o en copia oculta.
b) El correo remitido se recoge por el servidor MTA (Mail Transfer Agent) del usuario emisor, que se encarga de trasladarlo al servidor de correo entrante MDA (Mail Delivery Agent) del usuario destinatario. Este último almacena el

correo electrónico en tanto el usuario lo acepta. Los servidores de correo pueden ser propios, en el caso de empresas o instituciones (Guardia Civil, Policía, Ministerio de Justicia) o servidores web (Yahoo, Gmail, Microsoft) y siguen en su actuación diferentes protocolos (POP3 o IMAP) en función de los cuales se aplican reglas distintas acerca de la conservación de la información transmitida. Por ello, cuando se utilice este medio de trasmisión, es posible localizar copia del mensaje enviado no solo en poder del usuario remitente y del usuario receptor, sino también en los respectivos servidores de envío y de recepción, dependiendo de los criterios establecidos sobre almacenaje de los mismos

Finalmente, y en cuanto a la comunicación que se desarrolla a través de las plataformas de redes sociales (Facebook, Tuenti, Google +…), los parámetros a tener en cuenta presentan las siguientes características:

a) Los usuarios, además de mensajes de texto, pueden difundir a través de la red imágenes, fotos, vídeos y en general contenidos multimedia a los que pueden tener acceso una o más personas en función de la decisión que, en cuanto a la publicidad de contenidos, adopte el propio emisor.
b) A diferencia de los supuestos anteriores, toda la información y contenidos que el usuario "vuelca" en el sistema quedan almacenados en bases de datos gestionadas por los administradores de la red social durante periodos prolongados de tiempo. Incluso después de darse de baja una persona como usuario de una red determinada, la información aportada por el mismo podría ser localizada en dichas bases de datos, dependiendo de los criterios que sobre conservación de información tengan quienes gestionan la plataforma

Como ya se ha indicado, el problema que plantea la utilización como prueba de los soportes físicos o electrónicos con los que se pretende documentar la imagen correspondiente a una comunicación canalizada a través de cualquiera de estos medios, es la posibilidad de manipulación tanto en lo que se refiere a la propia existencia de la comunicación que se documenta como en cuanto al origen, destino o contenido de la misma. Las potencialidades y capacidades que ofrecen las herramientas TIC hacen posible la simulación total o parcial de dichos contenidos, lo que en muchas ocasiones determinará la necesidad de llevar a efecto una adecuada corroboración de estas evidencias a los efectos de hacer posible su eficacia en el proceso.

Así, es un hecho conocido que, sin necesidad de especiales conocimientos informáticos, es factible hacerse con el control de la cuenta de otro usuario; suplantar la identidad de terceras personas, simular el origen de una concreta comunicación o

incluso crear rastros ficticios de una transmisión, de tal forma que se pueda atribuir una persona un contacto en el que en realidad no haya participado. También estas herramientas permiten la modificación de contenidos de las comunicaciones realmente existentes mediante la alteración de mensajes por supresión o adición de frases o archivos adjuntos, alteración de fechas etc.

Tanto en el caso de que se impugnen las capturas de pantalla aportadas al procedimiento, como el propio archivo electrónico en el que se recoge el contenido cuestionado, podrá ser necesario practicar –según el extremo que se impugne- diligencias de prueba para acreditar la existencia de la comunicación, su origen, destino o contenido, pero no en todos los casos resultará imprescindible la realización de prueba pericial. Dicha diligencia sólo puede resultar inexcusable cuando no exista posibilidad de acreditar aquéllos extremos por otros medios, tales como la declaración de otros destinatarios de la comunicación, la aportación por el administrador de una red social, previa autorización judicial, del contenido cuestionado u otros. Incluso, cuando lo que se discuta sea la identificación del emisor de una comunicación, quizá sea suficiente la aportación de los datos de tráfico relativos a un determinado proceso comunicativo. Todo ello sin olvidar la posibilidad de que haya sido utilizada alguna forma mensajería electrónica certificada, circunstancia que solventará muchas de las dificultades planteadas.

Es de referencia obligada en esta materia lo establecido en el artículo 26 del C. Penal a cuyo tenor tiene carácter de documento *todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.* La doctrina del Tribunal Supremo, al respecto, se recoge nítidamente en la Sentencia de 18-XI-1998, que al comentar el sentido del precepto incorporado a la normativa penal sustantiva por el legislador de 1995 recuerda que *en el debate tradicional entre la concepción latina del documento que lo reduce a la forma escrita y la concepción germánica que admite cualquier base material susceptible de incorporar una declaración jurídicamente relevante escrita o no, la norma se inclina por la concepción germánica más amplia, como ya había efectuado antes un sector de la doctrina española y la jurisprudencia de esta Sala ( SS 19-4-1991; 20-·-1992 y 15-3-1994 entre otras): Cabe, en consecuencia cualquier soporte hábil (papel, piedra, madera, cinta magnetofónica, película cinematográfica, disco de ordenador etc.) para fijar datos jurídicamente relevantes, tanto a través de la escritura como de otros medios (fotográficos, cinematográficos, sonoros, informáticos, etc.).* En consecuencia, es evidente que un archivo electrónico debe ser considerado como un documento a la vista de esta definición, en el contexto del proceso penal.

Por su parte, el artículo 3.5 de la Ley de Firma electrónica 59/2003 de19 de diciembre considera documento electrónico *la información de cualquier naturaleza en*

*forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*

Frente a la ausencia de regulación acerca de esta materia en la Ley de Enjuiciamiento Criminal, tanto en lo que se refiere a la prueba documental como a la prueba en soporte electrónico, la Ley de Enjuiciamiento Civil, debido a su más reciente publicación, se ocupa de ello en el capítulo VI del Título I de su Libro II, bajo el epígrafe *De los medios de prueba y de las presunciones*

Concretamente, el artículo 299 de dicho texto legal, al relacionar los medios de prueba, incluye en su número 1, entre los de carácter tradicional, los documentos tanto públicos como privados y en su número 2, como medio de prueba diferente, se refiere a *los medios de reproducción de la palabra, el sonido y la imagen, así como a los instrumentos que permitan archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otras clase, relevantes para el proceso.* Estos últimos constituyen un *tertius genus* no fácilmente encuadrable como prueba testifical, ni documental ni pericial.

Si nos referimos a las conversaciones aportadas mediante impresiones o capturas de pantalla, puede considerarse que se trata de documentos privados que quedarían sometidos al régimen previsto en los artículos 324 y ss de la LEC. Concretamente el artículo 325 remite a su vez al art 268 en cuanto a la forma de presentación de los mismos, que habrá de hacerse con originales, con copia autenticada, o a través de imágenes digitalizadas indicando el apartado 2º de ese mismo precepto que *si la parte solo posee copia simple….podrá presentar esta, ya sea en soporte papel o mediante imagen digitalizada…, que surtirá los mismos efectos que el original, siempre que la conformidad de aquella con este no sea cuestionada por cualquiera de las demás partes.* Completa la regulación el apartado 3º del mismo artículo en el que se contempla la posibilidad de designar el expediente, protocolo, archivo o registro público, en que se encuentra el original del documento cuestionado

Por su parte el artículo 326 LEC se refiere a la fuerza probatoria de los documentos privados y dispone que cuando los mismos fueren impugnados, el que lo haya presentado podrá pedir un cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto, y si no lograra determinarse la autenticidad del documento o no se hubiera propuesto prueba alguna, se valorarán aquéllos conforme a la sana crítica.

En cuanto a los archivos electrónicos, es obvio que pueden ser incluidos en el apartado 2º del artículo 299 antes citado, de cuya regulación se ocupa la Ley de Enjuiciamiento Civil en la sección 8ª del mismo capítulo sexto que estamos analizando.

Así, el artículo 382 LEC, en el apartado 1º se refiere específicamente a la posibilidad de que las partes propongan *como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación u otros semejante,* indicando en su número 2º que quien efectúe esta propuesta también *podrá aportar los dictámenes o medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes o medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido.*

Por su parte el artículo 384-1º LEC contempla la posibilidad de que el Tribunal examine por sí mismo *los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas….que por ser relevantes para el proceso hayan sido admitidas como prueba,* permitiendo igual conocimiento a las partes, de tal forma que estas últimas puedan alegar y proponer lo que estimen conveniente al respecto. También en estos casos las partes podrán aportar dictámenes o medios de prueba a fin de acreditar/impugnar la autenticidad o exactitud del material aportado.

En uno y otro caso la valoración de estas pruebas queda sometida a las reglas de la sana critica (arts. 382.3 y 384.3 LEC)

No obstante, ha de indicarse que la LEC también se refiere específicamente a los archivos electrónicos como prueba documental, pero sólo les reconoce esta naturaleza cuando el documento electrónico aportado al procedimiento se encuentre firmado con firma electrónica. Efectivamente, el artículo 326 de la LEC, relativo a los documentos privados, indica que *cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo dispuesto en el artículo 3 de la Ley de Firma Electrónica*. Dicho artículo dispone en su apartado octavo que *el soporte en el que se hallen los datos firmados electrónicamente será admisible como prueba documental en un juicio* y el apartado cuarto dispone que *la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita respecto a los datos consignados en aquél*. De ello se deduce que sólo los archivos electrónicos firmados con firma electrónica reconocida tienen el mismo valor que si la firma fuera manuscrita, y puede ser considerado como prueba documental con todos los efectos que esa condición otorga conforme a lo dispuesto en los artículos 326 y 319 de la LEC. Si el archivo electrónico se encuentra firmado con cualquier otro tipo de firma electrónica, distinta a la firma reconocida, puede ser también aportado como prueba documental pero no gozará de la prevalencia probatoria de las anteriores en caso de impugnación. Por último, si el archivo electrónico no está firmado electrónicamente realmente no tiene la consideración de documento, sino que habrá de ser aportado

como uno de los medios de prueba que hemos denominado como *tertius genus* y previstos en el artículo 299.2 de la LEC.

En definitiva, y aplicando todos estos preceptos a la cuestión que nos ocupa, la impugnación de una evidencia de estas características exigirá -en atención a las circunstancias de cada supuesto y a salvo de aquellos casos en que su validez e integridad sea asumida por los intervinientes en el contacto[1] o resulte acreditada por otros medios- de la práctica de la actividad probatoria necesaria para corroborar la existencia de dicha comunicación, su origen y destino, la identidad de los interlocutores y el propio contenido de la misma. Cuáles sean las diligencias oportunas a realizar con dicha finalidad dependerá del medio tecnológico a través del cual se haya canalizado el contacto cuestionado, pues las específicas características técnicas de unos u otros sistemas de comunicación resultan determinantes para la constatación del hecho, el análisis de los metadatos de la transmisión, o la posibilidad de contrastar la evidencia presentada con el mensaje originalmente enviado y recibido.

En consecuencia y a partir de este planteamiento, es necesario analizar uno a uno los distintos sistemas de transmisión antes reseñados para concretar en cada supuesto cuáles serían los medios adecuados para corroborar -en caso de duda al respecto- la autenticidad o integridad de los mensajes o contenidos cuya transmisión se pretende acreditar en el proceso mediante la reproducción en documento físico de dichos contenidos o la presentación del dispositivo de comunicación mismo.

En el supuesto de que el contacto se haya producido través de Whatsapp o herramienta similar (Telegram, Line, Spotbross, WeChat…etc), como se trata de aplicaciones multiplataforma, las posibilidades de actuación pueden variar según cual sea la utilizada. En todo caso ha de recordarse que, en términos generales, los mensajes o el material remitido se conservan únicamente en los dispositivos implicados en la transmisión, en carpetas locales, o en archivos configurados en la nube por el propio usuario -a través de las correspondientes herramientas como, por ejemplo Google Drive- y accesibles únicamente desde dichos terminales siempre y cuando el titular no haya decidido eliminarlos. Los administradores de las aplicaciones únicamente conservan una información limitada acerca de datos de tráfico o los relativos a identificación de usuarios, numero de abonado telefónico o identificación de direcciones IP.

Es por ello que la forma de acreditar la propia existencia del mensaje y su contenido original conlleva efectuar las oportunas comprobaciones sobre los propios dispositivos utilizados en la transmisión. Dicha comprobación, en principio, puede realizarse a partir del aparato emisor si lo que interesa es comprobar el mensaje

[1] Tal y como acontece en las SSTS 300/2015

enviado o del receptor si lo que se pretende es corroborar el que ha sido recibido. En relación con ello, es importante recordar que en muchas ocasiones serán varios los implicados en esa comunicación, como ocurre cuando, por ejemplo, se trata de un mensaje difundido a través de un chat de grupo, supuesto en que todos los integrantes del colectivo tendrán a su disposición una copia del texto original enviado, lo que facilitará la comprobación del mismo.

Cuando existan sospechas de alteración, eliminación o simulación de un mensaje determinado será preciso acudir a las copias de seguridad en orden a corroborar el origen, destino, contenido o incluso la propia existencia de la comunicación cuestionada. Estas copias se realizan de forma automática y en momentos determinados preestablecidos, generalmente una vez al día, y se van almacenando en el propio dispositivo o, en su caso, en archivos en la nube por lo que pueden ser recuperadas con los procedimientos técnico-forenses oportunos, siendo factible, de esta forma, conocer los contenidos y datos de tráfico del mensaje original y cotejar la información así obtenida, con la derivada de las evidencias aportadas. No obstante, para su utilización a los efectos que aquí interesan, ha de tenerse en cuenta que la copia archivada reflejará los mensajes tal y como se encontraban en el momento en que se generó dicha copia, por lo que si la alteración o supresión de una determinada comunicación enviada o recibida se efectúa antes de iniciarse el proceso de copiado, la información y/o contenido previo a la alteración o modificación no quedará registrada y devendrá irrecuperable desde ese dispositivo.

En consecuencia, en muchos de estos casos la única posibilidad de corroborar la existencia misma y el contenido y alcance de la comunicación, sin perjuicio de la limitada información que en su caso pudieran facilitar los administradores de la aplicación, será el análisis pericial contrastado de los aparatos -al menos dos, de origen y destino- supuestamente utilizados en el proceso comunicativo.

Algo parecido ocurre cuando la prueba cuestionada se refiere a un mensaje transmitido por SMS o MMS que ha sido eliminado del terminal emisor o receptor. En estos supuestos la intervención en el proceso de comunicación de los operadores de telefonía permitirá acreditar la existencia misma de la comunicación, y los datos de tráfico asociados a la misma, a partir de la información almacenada por dichos operadores en aplicación de lo establecido en la ley 25/2007 de 18 de octubre de conservación de datos de las comunicaciones electrónicas, accesible previa autorización judicial y con los requisitos legales (art 588 ter j LEcrim y 6 y 7 Ley 25/2007) durante el plazo de un año.

Cuestión distinta es la posibilidad de recuperar el contenido del mensaje eliminado. El escaso periodo de tiempo durante el cual los operadores de telecomunicaciones conservan los mensajes enviados o recibidos -el mínimo

imprescindible para finalizar el proceso comunicativo- determina que solo con carácter muy excepcional sea posible su obtención por esta vía. Sin embargo, ha de recordarse que dichos mensajes, aun habiendo sido borrados por el usuario, se mantienen en la memoria del terminal utilizado durante un periodo de tiempo que variará según las circunstancias, pero que puede ser suficiente para permitir su recuperación mediante la utilización de técnicas forenses adecuadas para ello.

Si lo que se cuestiona es un correo electrónico aportado como prueba, la intermediación de los prestadores de servicios de correo contribuye sin duda a facilitar la constatación de la comunicación y de su contenido. Además de las comprobaciones directas en los dispositivos emisor y receptor es posible, en muchos casos, corroborar los mensajes a través de los servidores intervinientes en el proceso de transmisión, Así, numerosos servidores - particularmente si utilizan el protocolo IMAP- conservan copia de los mensajes y de la cabecera técnica de los mismos cuyo análisis puede ofrecer información de extraordinario interés sobre el origen y circunstancias de la comunicación y sobre su contenido original. La posibilidad de reclamar esta información de tales intermediarios se encuentra regulada específicamente en el artículo 588 ter j de la LECrim, contemplándose igualmente el deber de colaboración de los prestadores de servicios en el artículo 588 bis c-h) y el artículo 588 ter e) ambos del mismo texto legal. En el supuesto de que se trate de servidores de correo radicados fuera de nuestras fronteras dicha petición deberá seguir los trámites de las solicitudes de auxilio judicial internacional.

Finalmente, cuando se trata de una comunicación o de la difusión de una información o de un contenido a través de plataformas de redes sociales, la retirada del contenido por parte del usuario emisor -o incluso de la supresión misma de su perfil- no supone generalmente la imposibilidad de recuperación de los mismos.

Las especiales características y el sistema de funcionamiento de estas redes sociales determinan que mucha de la información que se “sube” por los usuarios a estas plataformas esté destinada a la difusión pública, ya que no en vano son estructuras ideadas y planificadas para facilitar la relación y el conocimiento entre las personas, si bien en las distintas aplicaciones se ofrecen posibilidades para crear espacios de privacidad en los que el acceso a la información queda limitado a aquellos otros usuarios que determina el titular del respectivo perfil. En términos generales las plataformas ofrecen tres niveles de privacidad/publicidad: a) accesibilidad a amigos; b) accesibilidad a amigos de amigos y c) accesibilidad plena a toda la red. Dependiendo por tanto de si un contenido se ha difundido públicamente, o si se ha mantenido en alguno de los espacios de privacidad, las posibilidades de contrastar su autenticidad e integridad variaran extraordinariamente. Efectivamente, un contenido que se ha difundido públicamente es posible que pueda ser corroborado a partir de información

facilitada por cualquiera de los usuarios de la red que hayan tenido acceso al mismo o incluso que lo hayan hecho propio incorporándolo a su propio perfil.

Pero, en cualquier caso, en estos supuestos, como anteriormente se ha indicado y sin perjuicio de las protestas que en relación con ello se vienen haciendo por las autoridades de protección de datos[2], lo cierto es que los prestadores de servicios de redes sociales conservan -justificándolo en argumentos de diversa índole- una buena parte de la información publicada en las respectivas plataformas. Así, según explican, pese a que un perfil haya sido eliminado conservan la información relacionada con el mismo durante un periodo aproximado de 90 días, por si el usuario desea activar de nuevo su contacto. Ello determina que sea posible obtener de los mismos, previa autorización judicial, dicha información conservada cuando ello fuera necesario para contrastar pruebas o evidencias aportadas por las partes en el curso de un proceso penal.

Al respecto resulta de interés traer a colación la posibilidad de solicitar de dichos proveedores de servicios la preservación de la información que posteriormente va a ser solicitada mediante autorización judicial para evitar que sea destruida y garantizar que quede disponible a efectos de la investigación criminal. El nuevo artículo 588 octies de la LECrim se refiere expresamente a ello y habilita tanto al Ministerio Fiscal como a la Policía Judicial en el ejercicio de sus funciones a emitir directamente, como medida de aseguramiento, dicha orden de conservación.

La dificultad, no obstante, puede venir determinada, por el hecho de que muchos de estos proveedores de servicio de la sociedad de la información tienen su sede fuera de nuestro país, generalmente en los EEUU, por lo que será necesario recurrir a solicitudes de auxilio judicial internacional. En relación con ello han de tenerse en cuenta las pautas generales de actuación establecidas en la guía práctica sobre preservación y obtención de datos en internet [3]

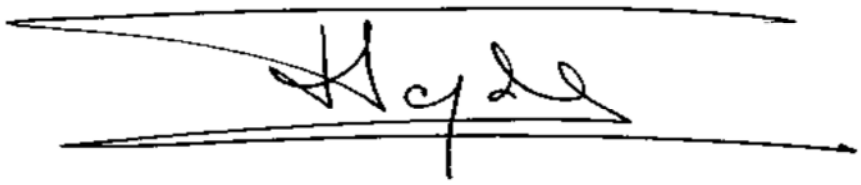
Sin perjuicio de lo anterior y a los efectos que nos ocupan, es interesante recordar que la posibilidad de llevar a efecto las correspondientes diligencias probatorias necesarias en cada caso a partir de los dispositivos utilizados en la transmisión dependerá, en la generalidad de los casos, de que los mismos estén a disposición de las autoridades judiciales y/o de los órganos de investigación desde la presentación de la denuncia. Por ello, la situación óptima es aquella en la que desde el momento inicial queda a disposición judicial el dispositivo a través del cual se ha canalizado la comunicación que pretende ser acreditada o, al menos, se lleva a efecto,

[2] Dictámenes 1/2008 y 5/2009 del Grupo de Trabajo del artículo 29

[3] Extraída del compendio de guías prácticas actualizado publicada por la Dirección General de Cooperación Jurídica Internacional del Mª de Justicia el 1 de octubre de 2015

con las debidas garantías, la identificación oportuna no solo del propio terminal sino también de las transmisiones objeto de prueba, a fin de garantizar la constancia en el procedimiento de los datos que individualizan el dispositivo o dispositivos concernidos, así como los de sus titulares/usuarios, perfiles utilizados, números de teléfonos asociados, terceros intervinientes si se trata de una comunicación múltiple, fecha y hora del contacto, archivos adjuntados…etc. Es por ello que los Sres. Fiscales, cuando el temprano conocimiento del inicio de la investigación lo permita, cuidarán de que se lleven a efecto estas diligencias para el debido aseguramiento del material probatorio que posteriormente pueda ser de utilidad en el proceso.

Madrid, a 30 de mayo de 2016



Elvira Tejada de la Fuente

Fiscal de Sala contra la Criminalidad Informática