



FERNANDEZADVOCATS

LA PRUEBA DIGITAL EN EL PROCESO PENAL

Un mensaje de Whatsapp, un correo electrónico, un audio, un vídeo o una publicación en redes sociales pueden ser decisivos en una investigación penal. A menudo contienen el primer indicio de un hecho, sitúan a una persona en una conversación relevante o permiten reconstruir una secuencia de acontecimientos.

Sin embargo, que una información aparezca en la pantalla de un teléfono no significa, por sí solo, que pueda fundar una condena.

La prueba digital plantea una dificultad singular: es extremadamente útil, pero también fácil de copiar, editar, recortar, reenviar, descontextualizar o atribuir a quien no la creó.

El proceso penal no desconfía de los medios electrónicos por ser electrónicos. Lo que exige es que puedan responderse, con garantías, cinco preguntas distintas: ¿se obtuvo lícitamente?, ¿es auténtica?, ¿está íntegra?, ¿se ha conservado correctamente?, ¿queda corroborada por el resto de la prueba?

La incorporación de esta clase de evidencias ha obligado a los tribunales a adaptar las reglas tradicionales de valoración de la prueba a una realidad tecnológica en constante evolución. La cuestión ya no consiste únicamente en determinar si un determinado archivo existe, sino si puede afirmarse con un grado suficiente de fiabilidad que ese archivo refleja fielmente la realidad de los hechos investigados. Precisamente por ello, la prueba digital exige un análisis especialmente riguroso, en el que confluyen cuestiones de legalidad procesal, garantías constitucionales, informática forense y valoración probatoria.

1. No toda prueba digital plantea el mismo problema

La expresión “prueba digital” comprende realidades muy distintas. Puede ser una conversación de Whatsapp o Telegram, un correo electrónico, una nota de voz, la



FERNANDEZADVOCATS

grabación de una llamada, una fotografía, un vídeo, una publicación en redes sociales, un historial de navegación, un documento almacenado en el ordenador o el contenido extraído de un teléfono móvil. A esta lista podrían añadirse también registros de geolocalización, archivos almacenados en la nube, registros de acceso a aplicaciones, comunicaciones efectuadas mediante plataformas de videoconferencia o cualquier otro dato generado o conservado en soporte electrónico.

Sin embargo, todas estas evidencias comparten únicamente su naturaleza digital. Desde un punto de vista probatorio, presentan características muy diferentes y, en consecuencia, no todos ofrecen el mismo grado de fiabilidad ni exigen idénticas cautelas para su incorporación al proceso penal.

No presenta el mismo punto de partida un archivo obtenido mediante una copia forense de un dispositivo intervenido judicialmente que una simple captura de pantalla remitida por una de las partes. Tampoco es equiparable un correo electrónico extraído directamente del servidor donde permanece almacenado con un documento impreso cuya procedencia resulta desconocida, ni un audio reconocido por quienes participaron en la conversación con una grabación cuyo origen no ha podido determinarse.

Resulta igualmente necesario diferenciar entre la prueba digital originaria y la prueba derivada de ella. La primera se identifica con el soporte original en el que se generó o almacenó la información —por ejemplo, el teléfono móvil, el ordenador o el servidor desde el que se obtuvo el archivo—. La segunda consiste en reproducciones posteriores, como capturas de pantalla, impresiones en papel, copias exportadas o archivos reenviados por aplicaciones de mensajería.

Esta distinción no implica que la prueba derivada carezca de valor probatorio. Sin embargo, cuanto mayor sea la distancia respecto del soporte original, mayor será normalmente la necesidad de acreditar la autenticidad, la integridad y la trazabilidad de la información aportada. Precisamente por ello, cuando la prueba digital adquiere una relevancia decisiva para la resolución del procedimiento, resulta aconsejable



FERNANDEZADVOCATS

preservar el dispositivo original o, al menos, obtener una copia forense que permita verificar posteriormente la ausencia de alteraciones.

Por ello, el análisis de la prueba digital debe realizarse siempre de forma individualizada. No basta con preguntarse si «existe un WhatsApp» o si «hay un correo electrónico». Es imprescindible determinar de qué dispositivo procede, quién lo aporta, cómo se obtuvo, si se conserva el soporte original, si la extracción respetó las garantías legales, si existe continuidad en la conversación, si pueden identificarse los interlocutores y si el contenido aparece corroborado por otros elementos de prueba.

En definitiva, la fiabilidad de una evidencia digital no depende únicamente del archivo en sí mismo, sino también de todo el proceso seguido desde su creación hasta su aportación al procedimiento judicial. Solo el examen conjunto de estas circunstancias permitirá al órgano judicial valorar correctamente su eficacia probatoria y determinar el peso que debe otorgársele dentro del conjunto de la actividad probatoria practicada.

2. Cinco conceptos que conviene no confundir

En la práctica forense, autenticidad, integridad y licitud son conceptos que suelen aparecer conjuntamente y, con frecuencia, se utilizan indistintamente. Sin embargo, responden a problemas completamente diferentes. Una prueba puede ser auténtica pero haberse obtenido ilícitamente; puede ser lícita pero encontrarse incompleta; o puede conservar íntegro su contenido sin que pueda acreditarse quién lo creó. Precisamente por ello conviene analizarlos separadamente.

2.1 Autenticidad: ¿quién creó o envió el contenido?

La autenticidad se refiere a la atribución. En una conversación de mensajería instantánea, la cuestión no es sólo que el texto aparezca bajo un nombre o un número de teléfono: debe poder sostenerse que procede realmente de la persona a la que se atribuye y que los interlocutores son quienes se dice que son.

Una cuenta puede ser utilizada por otra persona, un terminal puede ser compartido, un nombre de contacto puede modificarse y un perfil en redes



sociales puede ser falso. La identificación del emisor exige, según los casos, contrarrestar el teléfono, el dispositivo, los metadatos, el reconocimiento de los interlocutores, la prueba testifical y otros datos externos.

En la práctica, la autenticidad rara vez descansa sobre un único elemento. Lo habitual es que el tribunal construya su convicción a partir de un conjunto de indicios convergentes: el reconocimiento por los participantes, la coincidencia con otros documentos, los datos de geolocalización, las agendas de contactos, el contenido de otras comunicaciones o las propias circunstancias del hecho investigado.

2.2 Integridad: ¿el contenido se mantiene completo y sin alteraciones?

Un archivo puede ser auténtico y, aun así, estar incompleto o haber sido alterado. La integridad exige poder descartar adiciones, eliminaciones, cortes, modificaciones de fechas y horas, manipulación de adjuntos o selección sesgada de una conversación.

Una captura asilada revela sólo lo que muestra esa imagen. Puede omitir mensajes anteriores, respuestas posteriores o elementos de contexto. De ahí que el acceso al hilo completo y al dispositivo original, cuando sea posible, tenga un valor muy superior.

2.3 Licitud: ¿se obtuvo respetando los derechos fundamentales?

La prueba puede ser auténtica e íntegra, pero no ser utilizable si se obtuvo vulnerando derechos fundamentales. El caso paradigmático es el acceso al contenido de un móvil, ordenador, cuenta de correo o aplicación de mensajería sin la cobertura legal exigible.

El art. 588 sexies a de la LECrim exige, como regla general, autorización judicial para el acceso a los datos o archivos almacenados en dispositivos electrónicos intervenidos. La STS 489/2018, de 23 de octubre, subraya, en esa línea que la mera incautación de un dispositivo no habilita automáticamente para examinar su contenido. En el ámbito de una investigación judicial, el acceso a datos y



comunicaciones exige la autorización judicial y los requisitos legalmente establecidos, salvo supuestos excepcionales que deben justificarse.

Es importante diferenciar ese supuesto de la grabación realizada por uno de los propios participantes en una conversación. No toda grabación es ilícita por el hecho de no haber sido anunciada. La respuesta depende de quién graba, qué conversación se registra, qué acceso se produce y qué derecho fundamental puede verse afectado. La licitud debe analizarse siempre con el caso concreto.

3. WhatsApp, Telegram y las capturas de pantalla

La jurisprudencia del Tribunal Supremo ha fijado una pauta especialmente relevante para los mensajes de mensajería instantánea. La STS 300/2015, de 19 de mayo, advirtió sobre la facilidad de manipulación de los archivos digitales y señaló que, si se impugna la autenticidad de una conversación aportada mediante impresiones o pantallazos, quien pretende beneficiarse de ella debe acreditar suficientemente su idoneidad. EN ese escenario, la pericial informática puede ser necesaria para identificar origen, interlocutores e integridad.

Ahora bien, esta doctrina no significa que todo Whatsapp sea falso hasta que un perito diga lo contrario. La STS 375/2018, de 19 de julio, introdujo una precisión decisiva: no existe una presunción general de falsedad de los mensajes digitales ni una exigencia automática de pericia en todos los casos.

Ello es coherente con el principio de libre valoración de la prueba previsto en el proceso penal. El juez no atribuye automáticamente un determinado valor a una conversación de WhatsApp, sino que la examina conjuntamente con el resto del material probatorio disponible. En consecuencia, un mismo mensaje puede resultar insuficiente en un procedimiento y plenamente convincente en otro si aparece corroborado por declaraciones testificales, documentos, informes periciales u otros elementos objetivos.

La necesidad de una comprobación técnica se intensifica cuando la impugnación es concreta y razonada. No tiene el mismo alcance afirmar de forma genérica «esa



FERNANDEZADVOCATS

conversación está manipulada» que señalar que falta parte del hilo, que el número no pertenece al supuesto emisor, que el teléfono fue usado por varias personas, que las horas son incompatibles con otros datos objetivos o que la copia no coincide con el terminal original.

Por eso, una mera captura puede tener valor orientativo o corroborador, pero resulta débil cuando es la única prueba de cargo y se discute seriamente su procedencia o contenido. La fuerza aumenta, en cambio, si se aporta el terminal original, se visualiza la conversación completa, se realiza un cotejo técnico, los interlocutores reconocen los mensajes o existen elementos externos que confirman su contenido.

4. Correos electrónicos, audios vídeos, redes sociales y metadatos.

Los correos electrónicos plantean la misma necesidad de atribución. Que un mensaje provenga de una dirección aparentemente identificable no prueba por sí solo quién lo escribió ni que su contenido no haya sido alterado. Pueden ser relevantes los encabezados técnicos, la trazabilidad del envío, los servidores, los archivos adjuntos, la cuenta desde la que se remitió y la relación del correo con otras actuaciones verificables.

En los audios y vídeos hay que distinguir, además, dos planos. El primero es la identificación de voces, imágenes y participantes. El segundo es la integridad del archivo: si se produjo una edición, un corte o una modificación. Cuando la discusión es relevante, la pericial puede analizar el soporte, la existencia de alteraciones, la continuidad de la grabación y los datos técnicos disponibles.

Las publicaciones de redes sociales presentan riesgos adicionales: perfiles suplantados, modificaciones posteriores, contenidos efímeros y capturas que no permiten conocer la URL, fecha, contexto o identidad real del usuario. Una impresión de una publicación puede ser útil, pero conviene preservarla junto con el enlace, el perfil, la fecha visible y, cuando el caso lo requiera, una verificación técnica o una constatación formal.



FERNANDEZADVOCATS

Asimismo, en muchas ocasiones la mayor fuerza probatoria de un archivo digital no reside únicamente en su contenido, sino en la información técnica que lo acompaña.

Los denominados metadatos pueden aportar información relativa a la fecha de creación, modificaciones posteriores, dispositivo utilizado, localización, formato del archivo o aplicación empleada para su generación. Aunque no siempre están disponibles, cuando pueden preservarse constituyen un importante elemento de corroboración de la autenticidad y de la integridad de la prueba.

La informática forense concede una especial relevancia a estos datos porque permiten verificar extremos que difícilmente pueden apreciarse mediante una simple visualización del archivo. En consecuencia, cuanto antes se preserve el soporte original, mayores serán las posibilidades de conservar también esta información técnica.

5. Impugnación de dichas pruebas en sede de procedimiento penal

Impugnar una prueba digital no equivale a negar su existencia. La impugnación eficaz debe identificar el problema concreto: origen desconocido, falta del dispositivo, ausencia de continuidad, posible edición, incoherencia temporal, perfil suplantado, acceso ilícito o quiebra de la cadena de custodia.

La objeción más fuerte de quien aporta un archivo es que la otra parte se limita a formular dudas genéricas para debilitar una evidencia incómoda. La réplica debe ser precisa: si la crítica se apoya en datos verificables y el archivo es decisivo, será razonable solicitar comprobación técnica, cotejo con el original o contradicción pericial.

En sentido inverso, quien aporta la prueba no debería confiar en que un pantallazo aislado bastará siempre. Si anticipa que la autenticidad será discutida, debe procurar aportar el soporte original, solicitar las diligencias adecuadas y reforzar el contenido con elementos externos de corroboración.

6. Conclusiones



FERNANDEZADVOCATS

La prueba digital ocupa ya un lugar central en los procedimientos penales. Pero su utilidad no depende de acumular capturas, sino de poder acreditar *su origen, su conservación, su integridad, su obtención lícita y su conexión con el hecho investigado.

Un WhatsApp, un correo, un audio o una publicación en red social pueden ser prueba eficaz. También pueden ser insuficientes si se presentan de forma descontextualizada, sin soporte original o frente a una impugnación técnica fundada. La prudencia exige no confundir la existencia de un contenido en una pantalla con su eficacia probatoria.

En proceso penal, la mejor evidencia digital es la que permite al tribunal responder con seguridad a una pregunta esencial: ¿podemos confiar en que este archivo es lo que dice ser y que expresa, completo y sin alteraciones, lo que realmente ocurrió?

La creciente digitalización de las relaciones personales y profesionales hace prever que este tipo de evidencias será cada vez más frecuente en los procedimientos penales. Ello obligará a abogados, fiscales y tribunales a familiarizarse con conceptos técnicos que hace apenas unos años resultaban ajenos al proceso judicial.

En definitiva, la prueba digital no constituye una categoría probatoria privilegiada ni sospechosa por naturaleza. Debe someterse al mismo juicio crítico que cualquier otro medio de prueba, si bien atendiendo a las particularidades derivadas de su soporte tecnológico. Solo cuando concurren autenticidad, integridad, licitud y una adecuada corroboración podrá alcanzar la fuerza necesaria para fundamentar una condena o sustentar una absolución.

**El presente artículo es meramente divulgativo y no supone asesoramiento ni compromiso de actualización.*

Para más información o asesoramiento, contacte con info@fernandezadvocats.es.