Capítulo 18

La prueba de la violencia de género digital en el proceso penal de menores[1]

Pablo Grande Seara

Profesor Titular de Derecho Procesal
Universidad de Vigo

I. INTRODUCCIÓN

La llamada violencia de género digital o ciberviolencia de género se puede definir como la violencia psicológica ejercida sobre la mujer por quien sea o haya sido su cónyuge o pareja de hecho, aún sin convivencia, a través de cualquier medio tecnológico o digital, mediante conductas en el plano virtual consistentes en injurias, coacciones, amenazas, humillaciones o vejaciones, exigencia de obediencia o sumisión, o limitaciones de su ámbito de libertad[2].

1. Este trabajo ha sido elaborado en el marco del proyecto de investigación "Respuesta jurídica y socioeducativa a la violencia de género ejercida por menores. Protección de la víctima e intervención con el menor agresor", subvencionado por el Ministerio de Ciencia e Innovación, Proyectos de I+D+I" dentro de los Programas Estatales de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+I y de I+D+I orientada a los Retos de la Sociedad en la convocatoria de 2019, (Ref. PID2019-106700RB-I00).

2. La DELEGACIÓN DEL GOBIERNO CONTRA LA VIOLENCIA DE GÉNERO, (https://violenciagenero.igualdad.gob.es/informacionUtil/comoDetectarla/VG_Digital/home.htm), destaca diez signos que podrían indicar que se está produciendo violencia digital: "acosar o controlar a tu pareja usando el móvil; interferir en relaciones de tu pareja en Internet con otras personas; espiar el móvil de tu pareja; censurar fotos que tu pareja publica y comparte en redes sociales; controlar lo que hace tu pareja en las redes sociales; exigir a tu pareja que demuestre dónde está con su geolocalización; obligar a tu pareja a que te envíe imágenes íntimas; comprometer a tu pareja para que te facilite sus claves personales; obligar a tu pareja a que te muestre un chat con otra persona; mostrar enfado por no tener siempre una respuesta inmediata online".

Este tipo de violencia de género es la más común en el caso de los jóvenes y adolescentes, incluso a veces sin ser conscientes de ello; e incluye, entre otras, las siguientes conductas:

- *Haching* o intrusismo informático, es decir, el espionaje dentro de la pareja. Implica acceder al teléfono móvil u otro dispositivo digital de la pareja para conocer el contenido o los destinatarios de sus conversaciones o mensajes, ejerciendo así un control sobre ella.
- *Sexting*, que consiste en la difusión de imágenes (fotos o vídeos) de carácter erótico o sexual, tomadas por el agresor o grabadas por la propia víctima, para dañar el honor o la imagen de ésta.
- *Sextorsión* o extorsión sexual, que consiste en el chantaje a la víctima para que realice una determinada acción, bajo amenaza de publicar o compartir imágenes íntimas que el extorsionador tiene de ella.
- *Ciberstalking,* que es el acoso a través de medios telemáticos o redes sociales. El acosador, de forma insistente y reiterada, e incluso intimidatoria, intenta establecer contacto telemático con la víctima contra su voluntad, limitando así su capacidad de obrar o generándole sentimiento de inseguridad.
- *Ciberbullying*, que supone una situación de hostigamiento, abuso y vejación a la víctima, de forma sostenida y repetida a lo largo del tiempo. Puede adoptar formas muy heterogéneas, como, por ejemplo, enviar mensajes amenazantes a la víctima; crear un perfil falso de la víctima a través del que demanda contactos sexuales; seguir a la víctima en lugares de internet a los que accede habitualmente; dar de alta el mail de la víctima en determinados lugares de internet para que reciba spam; difundir rumores sobre la conducta de la víctima para que otras personas le acosen; etc.

Según se hace constar por el OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, en su informe *Violencia digital de género: una realidad invisible*, el primer problema a la hora de analizar y abordar esta violencia de género digital en España, y en la UE, es la escasez de estadísticas, por lo que, en consecuencia, se sabe muy poco sobre el porcentaje real de las víctimas y de la prevalencia de los daños causados. Y añade que esta escasez de estadísticas "deriva de la dificultad de medir y cuantificar un fenómeno tan complejo, principalmente porque en la mayoría de los países no están tipificados como delito todas las formas de ejercer violencia digital contra las mujeres, de ahí que los datos policiales o de los organismos judiciales sean muy limitados"[3].

3. *Vid.*, OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, *Violencia digital de género: una realidad invisible*, https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/220429_i_InformeONTSI.pdf, p. 8.

Con todo, en este informe se reflejan algunos datos que ponen de manifiesto la dimensión del problema entre las jóvenes. Se destaca que la edad es un factor determinante que incrementa las posibilidades de experimentar acoso en internet porque las más jóvenes también son las que más utilizan los servicios digitales. Así se puede constatar en los siguientes datos: más de un 25% de las mujeres entre 16 y 25 años en España han recibido insinuaciones no apropiadas a través de redes; más del 20% de las jóvenes entre 16 y 20 años ha recibido correos electrónicos, mensajes de texto o fotografías sexualmente explícitas que les hicieron sentirse ofendidas, humilladas o intimidadas; y, en menos de una década, se han multiplicado por cinco en España los delitos de contacto mediante tecnología con menores de 16 años con fines sexuales. Además, de las niñas y jóvenes que han sufrido acoso online, el 42% mostraron estrés emocional, baja autoestima y pérdida de confianza; el 24% se sintieron inseguras físicamente; y el 19% tuvo problemas con las amistades y la familia, y el 18%, en el colegio o instituto[4].

Como se puede comprender, estas conductas delictivas que integran la violencia de género digital se pueden cometer y, en su caso, tratar de probar, utilizando distintos medios o sistemas de comunicación electrónica, es decir, distintas tecnologías de la información y la comunicación (TIC´s), siendo los más comunes el correo electrónico, los mensajes SMS o multimedia (MMS), las aplicaciones de mensajería instantánea, bidireccional o multidireccional (Whatsapp, Telegram, Line,…), o las plataformas de redes sociales (Facebook, Instagram, Twiter, Youtube, Tiktok,…).

Cada una de estas tecnologías de comunicación presenta características técnicas distintas, lo que, por supuesto, tendrá consecuencias a efectos de su utilización como fuente de prueba en un proceso penal, especialmente, en lo relativo a su valoración probatoria en el caso de que la parte contraria cuestione la autenticidad de su autoría o la integridad de su contenido. Así, por ejemplo, los mensajes de Whatsapp no se guardan en un servidor del proveedor del servicio, sino únicamente en los terminales de emisión y recepción, por lo que no permite solicitar a aquel que certifique el contenido de los mensajes enviados o recibidos para su cotejo con los aportados al proceso; lo que sí es posible en el caso de la comunicación a través de redes sociales, ya que los contenidos que se suben a la red quedan almacenados en servidores de los administradores de la red social durante un tiempo[5].

4. *Vid*., OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, *Violencia digital de género…, op. cit*., pp. 9 a 13.
5. *Vid*., FISCALÍA GENERAL DEL ESTADO, *Dictamen 1/2016, sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportados al proceso penal como*

Pero, a fin de delimitar y centrar más el tema de este trabajo, conviene destacar también que, precisamente, por sus características técnicas particulares, el uso de estas tecnologías de la comunicación se ha ido "especializando" en función del tipo de relaciones interpersonales para las que se utilizan y del perfil de usuarios más habituales. Buena muestra de ello es que, por ejemplo, el correo electrónico está quedando cada vez más relegado a un tipo de comunicación que podemos calificar como más profesional o formal; mientras que las aplicaciones de mensajería instantánea y las plataformas de redes sociales (en parte, por ser más fácilmente accesibles a través de un *smartphone*) se utilizan para las relaciones de tipo más personal e informal[6], y, en particular, entre los usuarios más jóvenes. Por ello, son estos últimos los sistemas de comunicación más propicios y habituales para la comisión de este tipo de violencia de género digital que se puede investigar y enjuiciar en el proceso penal de menores.

Por esta razón, en este trabajo, me centraré en la problemática procesal que suscita el uso en el proceso penal de estas dos fuentes de prueba: los mensajes (de texto, voz, imagen o vídeo) emitidos y recibidos a través de aplicaciones de mensajería instantánea y los mensajes o comunicaciones transmitidos a través de plataformas de redes sociales. Y tal problemática afecta, en mayor o menor medida, a lo que podemos llamar las "tres fases de la prueba electrónica o digital", a saber, la licitud de la obtención de la fuente de prueba, el medio de prueba a través del cual se pueden aportar o incorporar al proceso estas fuentes de prueba digitales, y, finalmente, la valoración probatoria de estas fuentes de prueba, en particular, en el caso de que la contraparte la impugne por cuestionar la autoría (autenticidad) o integridad (contenido) de la misma.

II. LICITUD DE LA OBTENCIÓN DE LA FUENTE DE PRUEBA DIGITAL

Como se comprenderá, las dudas que se pueden suscitar sobre la licitud en el modo de acceso y obtención de las fuentes de prueba electrónicas o digitales, y su consiguiente validez o no como fuente de prueba en un proceso penal, se refieren, básicamente, a las fuentes de prueba que hayan sido obtenidas y aportadas al proceso por las propias partes. Por

---

medio *de prueba de comunicaciones electrónicas* http://milansabogados.com/wp-content/uploads/2018/05/Dictamen-n%C2%BA-1-2016-sobre-el-valor-probatorio-de-las-capturas-de-pantallas.-Unidad-Criminalidad-Informa%CC%81tica.pdf.

6. *Vid.*, FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías", *Revista General de Derecho Procesal,* 44 (2018), p. 17.

lo general, no se plantean tales cuestiones de licitud cuando se trata de evidencias digitales obtenidas como consecuencia de una intervención policial acordada en el marco de un proceso penal, siempre que ésta se desarrolle conforme a lo previsto legalmente (arts. 588 bis a) a 588 ter m)[7]; y arts. 588 sexies a) a 588 octies LECrim[8]). Además, teniendo en cuenta que, normalmente, el tipo de delitos a los que nos estamos refiriendo son de carácter semipúblico, la presentación de denuncia por la víctima dará lugar con cierta frecuencia a la práctica de tales diligencias policiales de investigación tecnológica, sin perjuicio de la colaboración o facilidades que pueda proporcionar ésta a tal fin, por lo que tampoco será muy habitual que la parte contraria pueda impugnar con fundamento la licitud de estas fuentes de prueba.

En cualquier caso, a la hora de analizar la licitud de la obtención por las partes de los mensajes y comunicaciones electrónicas y su validez como fuente de prueba a efectos de acreditar conductas de violencia de género digital en un proceso penal, debemos partir de cuáles son los derechos fundamentales que se pueden ver afectados y hasta qué punto admiten limitaciones. Tales derechos son el derecho al secreto de las comunicaciones privadas (art. 18.3 CE) y/o el derecho a la intimidad personal (art. 18.1 CE)[9].

El derecho al secreto de las comunicaciones privadas protege el proceso de comunicación frente a cualquier intromisión ajena, tanto por parte de autoridades públicas como de particulares, y alcanza a cualquier forma y canal de comunicación. Este derecho protege el proceso de comunicación, no sólo el contenido de la misma (es decir, los mensajes que se transmiten), y, por tanto, impide que un tercero pueda interceptar cualquier dato o elemento privado de la comunicación, como son los datos identificativos

7. En ellos se regulan las siguientes actuaciones: Disposiciones comunes a todas las diligencias de investigación tecnológicas (arts. 588 bis a) a 588 bis k) LEcrim); la interceptación de comunicaciones telefónicas y telemáticas (arts. 588 ter a) a 588 ter i) LECrim); la incorporación al proceso de datos electrónicos de tráfico (arts. 588 ter j) LECrim); y el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (arts. 588 ter k) a 588 ter m) LECrim).

8. En ellos se regulan el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) a 588 sexies c) LECrim); los registros remotos sobre equipos informáticos (arts. 588 septies a) a 588 septies c) LECrim); y las medidas de aseguramiento (art. 588 octies LECrim).

9. ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, Whatsapp, redes sociales): entre la insuficiencia y la incertidumbre", *IDP, Revista de Internet, Derecho y Política*, núm. 27, septiembre, 2018, pp. 71 y 72; RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas en los procesos de familia", en (Dir., Picó i Junoy, J y Abell Lluch, X.) *Problemática actual de los procesos de familia. Especial atención a la prueba*, Bosch, Barcelona, 2018, pp. 219 a 228.

de los intervinientes en la comunicación, la ubicación de estos, el tiempo y duración de la comunicación, o el tipo y contenido de la misma.

Esto significa que, por ejemplo, se vulnere este derecho al secreto de las comunicaciones por el mero hecho de que un tercero acceda a la cuenta de correo o a la aplicación de mensajería instantánea sin el consentimiento de su titular, aunque no pueda acceder o llegar a conocer el contenido de los mensajes[10]. En cambio, no se vulnera este derecho cuando el que utiliza o aporta al proceso datos de una comunicación es uno de los intervinientes en la misma; y ello con independencia del número de interlocutores que hayan participado en ella (por ejemplo, mensajes recibidos en un grupo de Whatsapp). La utilización o difusión de esos mensajes u otros datos de la comunicación por uno de los interlocutores podrá afectar, en su caso, al derecho a la intimidad, pero no al secreto de las comunicaciones.

A su vez, el derecho a la intimidad supone la existencia de un ámbito propio y reservado de una persona frente a la acción y el conocimiento de los demás. Pero es éste un derecho flexible, ya que su contenido y alcance se puede modular en función de la voluntad o conducta de su titular y de las circunstancias concurrentes en cada caso. Es decir, corresponde a cada persona acotar el ámbito de intimidad personal y familiar que quiere reservar al conocimiento ajeno. Por ello, el consentimiento (expreso o tácito) del titular permite la inmisión lícita en dicho ámbito.

Esto tiene particular importancia en el contexto familiar o de pareja, ya que las especiales relaciones de confianza que, normalmente, existen en este ámbito, al menos mientras no hay conflicto, así como el debido ejercicio de los derechos y deberes paternofiliales, hace que los límites de este derecho a la intimidad aparezcan a veces muy difuminados. Por ejemplo, como veremos, se entiende que no se vulnera este derecho a la intimidad con el uso por un miembro de la pareja de aquellos dispositivos o aplicaciones de comunicación que comparten de mutuo acuerdo (aunque ninguno de ellos podrá hacer un uso ilícito de los contenidos o de la información de la aplicación que perjudique a los demás usuarios). De igual modo, la jurisprudencia ha admitido como lícito el acceso por parte de un progenitor a los mensajes albergados en el teléfono móvil de su hijo menor de edad cuya custodia comparte, por entender que la vigilancia del uso que hace éste de las redes sociales entra dentro de sus obligaciones inherentes a la patria potestad previstas en el art. 154 CC[11].

Por tanto, no cabe duda de que estos derechos al secreto de las comunicaciones privadas y a la intimidad personal también rigen y han de ser

10. SAP de Illes Balears 431/2017, de 5 de septiembre (JUR 2017, 276317).
11. AAP de Pontevedra 893/2017, de 25 de octubre (JUR 2017, 308428)

respetados en el ámbito familiar o de pareja. Pero el contenido y efectividad de tales derechos se puede ver atenuado o difuminado por la "auto-renuncia" de sus titulares como consecuencia de la relación de confianza que suele existir en este contexto. Por ello, a efectos de determinar la licitud del acceso y obtención de mensajes y comunicaciones electrónicas para su aportación como fuente de prueba en un proceso penal por violencia de género digital, debemos distinguir diversos supuestos, según que la parte que los aporta haya sido o no emisora o receptora de los mismos[12].

1. OBTENCIÓN Y APORTACIÓN AL PROCESO DE COMUNICACIONES ELECTRÓNICAS RECIBIDAS POR LA PARTE PROCESAL

La obtención y aportación al proceso de mensajes y comunicaciones electrónicas recibidas por la propia parte no plantea, *a priori*, problemas de licitud, ya que, como se indicó, cualquiera de los interlocutores en la comunicación puede obtener y aportar lícitamente al proceso estos mensajes sin que se pueda entender vulnerado el derecho al secreto de las comunicaciones; y ello, aunque no sea el destinatario exclusivo de los mensajes en cuestión. Por ejemplo, tratándose de un mensaje recibido en un grupo de WhatsApp o a través de un correo electrónico enviado a un colectivo, cualquiera de los receptores puede aportar lícitamente al proceso dicho mensaje.

En este sentido, es clara la SAP de Asturias 280/2018, de 29 de junio, al señalar que "quien graba una conversación de otro atenta contra el derecho al secreto de las comunicaciones; pero quien graba una conversación con otro, no incurre en esta infracción, porque no hay secreto para aquel a quien la conversación se dirige"[13]. Por ello, concluye que no existe prueba ilícita cuando una parte aporta al proceso archivos de audio de conversaciones mantenidas con terceros en calidad de interlocutor.

Es más, sería lícita incluso la obtención y aportación de los mensajes al proceso por la persona titular del dispositivo electrónico en el que se han recibido tales mensajes, aunque no fuese ella directamente la destinataria de los mismos. Por ejemplo, cuando en la comunicación se utiliza el dispositivo o aplicación de mensajería de otra persona que luego encuentra dichos mensajes, o cuando, por error, se envían al destinatario

12. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, pp. 228 a 232.
13. SAP de Asturias 280/2018, de 29 de junio (JUR 2018, 240840).

equivocado. En este sentido, declara la SAP de Madrid 702/2015, de 24 de noviembre, que no concurre causa de nulidad porque los mensajes "han sido aportados al proceso por la propia persona titular del dispositivo electrónico que ha recibido los mensajes"[14].

En definitiva, la aportación al proceso como fuente de prueba de los mensajes y comunicaciones electrónicas que ha recibido la propia parte que los aporta es lícita ya que no vulnera el derecho al secreto de la comunicación, en tanto que la parte es interlocutora en la comunicación o titular del dispositivo o aplicación desde el que se transmite o recibe el mensaje. Y, en principio, la utilización de estas comunicaciones como fuente de prueba en un proceso, tampoco vulnera el derecho a la intimidad, siempre que el contenido de las mismas sea útil y pertinente (necesario) para probar hechos relevantes en el proceso[15].

2. OBTENCIÓN Y APORTACIÓN AL PROCESO DE COMUNICACIONES ELECTRÓNICAS TRANSMITIDAS O RECIBIDAS POR LA PARTE CONTRARIA O POR UN TERCERO

La licitud de la obtención y aportación al proceso como fuente de prueba de comunicaciones electrónicas transmitidas o recibidas por la parte contraria o un tercero queda supeditada a que se hayan respetado el derecho al secreto de las comunicaciones y el derecho a la intimidad de los interlocutores. Pero esto no significa que, en ningún caso, una parte pueda obtener y aportar lícitamente al proceso mensajes o comunicaciones de los que no es interlocutora. A este respecto, la doctrina y la jurisprudencia ha hecho algunas matizaciones

Por supuesto, no es admisible ningún tipo de interceptación por la parte de las comunicaciones de otra persona (sea la otra parte o un tercero) para poder aportarlas al proceso como fuente de prueba[16]; y ello,

14. SAP de Madrid 702/2015, de 24 de noviembre (ARP 2015, 1313).

15. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 231.

16. *Vid.*, SAP de Asturias 39/2017, de 15 de febrero (ARP 2017, 412). Como señala CUAIRÁN ("La aportación de WhatsApp como medio de prueba en el procedimiento penal", *Diario La Ley*, n.º 9219, Sección Tribuna, 15 de junio de 2018 (La Ley 5337/2018), p. 2), el acceso no consentido a conversaciones de terceros podría vulnerar el derecho fundamental a la intimidad y/o al secreto de las comunicaciones, lo que conllevaría que, además de ser considerada como prueba ilícita, dicha conducta fuera constitutiva de un delito de descubrimiento y revelación de secretos previsto y penado en el art. 197 CP. En el mismo sentido, DELGADO MARTÍN, J., "La prueba del Whatsapp", *Diario La Ley*, n.º 8605, Sección Tribuna, 15 de septiembre de 2015 (La Ley 5350/2015), p. 1.; MAGRO SERVET, V., "¿Cómo aportar la prueba digital en el

aunque exista vínculo personal o afectivo de especial confianza con el interviniente en la comunicación. La intervención de las comunicaciones, únicamente, está permitida cuando exista una resolución judicial que la autorice en el contexto de una investigación penal y con los límites y condiciones legalmente previstos (arts. 588 bis a) y ss. LECrim).

En cambio, no existe impedimento para obtener y aportar al proceso datos personales (por ejemplo, ubicación, fotografías) y comunicaciones de terceros (mensajes de texto, audio o video) a los que se puede acceder en abierto a través de internet. Los titulares de perfiles en la red pueden establecer los niveles de privacidad que quieren aplicar[17]. Por tanto, si establecen un nivel de libre acceso, sea absoluto o limitado, a su perfil, cualquier usuario de la aplicación que tenga autorizado el acceso al mismo podrá acceder y obtener copias de sus contenidos para aportarlos lícitamente al proceso[18].

En este sentido, las SSTS 292/2008, de 28 de mayo y 1299/2011, de 17 de noviembre, señalan que, efectivamente, las comunicaciones a través de internet se encuentran protegidas por el derecho al secreto del art. 18.3 CE; pero siempre que quede constatada la voluntad de los interlocutores de realizar dicha comunicación en el ámbito de la privacidad y en el ejercicio de su derecho a la intimidad, excluyendo toda injerencia de terceros en dicha comunicación, lo que habrá que valorar atendiendo a las circunstancias de cada caso concreto. Y no parece que tal voluntad exista cuando es el propio comunicante el que permite que sus mensajes y comunicaciones sean conocidos por terceros[19].

Un tercer supuesto, que se plantea de modo relativamente frecuente en el ámbito familiar y de pareja, es el de los dispositivos y aplicaciones de mensajería compartidos, o de titularidad personal, pero con acceso y uso autorizado a otros miembros del núcleo familiar. Por ejemplo, la pareja o los miembros de la unidad familiar comparten el uso del ordenador, la

---

proceso penal?", *Diario La Ley*, n.º 9824, Sección Doctrina, 7 de abril de 2021 (La Ley 3855/2021), p. 8.

17. Por lo general 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 (*Vid*., FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit*., p. 11).

18. Como señala ARMENTA DEU ("Regulación legal y valoración probatoria de fuentes de prueba digital…", *op. cit*., p. 74), la información insertada voluntariamente en la red para ser compartida con otros usuarios no goza de la protección del secreto de las comunicaciones; sin embargo, en supuestos como la información transmitida entre un grupo limitado o identificado de interlocutores sí resulta aplicable el art. 18.3 CE.

19. *Vid*., SSTS 292/2008, de 28 de mayo (RJ 2008, 3241) y 1299/2011, de 17 de noviembre (RJ 2012, 1540).

Tablet, una cuenta de correo electrónico, o una aplicación bancaria; y lo mismo cabe decir de los grupos de Whatsapp. En estos casos, se considera lícito que cualquiera de los sujetos autorizados para el uso de estos dispositivos o aplicaciones pueda acceder a ellos y obtener los mensajes y comunicaciones transmitidos o recibidos a través de los mismos. No se vulnera con ello el derecho al secreto de la comunicación porque todos han aceptado, expresa o tácitamente, el acceso de los demás sujetos autorizados. Ahora bien, podría vulnerarse el derecho a la intimidad si la información personal de alguno de los sujetos autorizados así obtenida se utiliza con fines ilícitos, para causarle un perjuicio[20]; lo cual no es el caso de que se utilice como fuente de prueba en un proceso penal.

Otro supuesto que también se da con frecuencia en el ámbito familiar es el del acceso por parte de un progenitor a los mensajes albergados en los dispositivos o aplicaciones de sus hijos menores de edad. En este sentido, la jurisprudencia ha admitido como lícito el acceso del progenitor a los mensajes albergados en el teléfono móvil de su hijo menor de edad, especialmente, cuando es el propio progenitor el que asume los gastos del dispositivo y de la conexión a internet, por entender que la vigilancia por los padres de la actividad en las redes sociales de los hijos menores de edad se incluye entre las obligaciones inherentes a la patria potestad del art. 154 CC.

Así, el AAP de Pontevedra 893/2017, de 25 de octubre, ante la denuncia presentada por la madre contra el padre, porque éste se habría apoderado de las conversaciones que mantuvo su hija a través de su teléfono móvil con su progenitora y denunciante, ha considerado lícito que, en virtud de este deber del padre conforme al art. 154 CC, que comparte con la denunciante la patria potestad de su hija menor, éste haya revisado en presencia de la hija determinadas conversaciones de Whatsapp mantenidas por ésta[21].

Finalmente, también se considera lícita la aportación al proceso como fuente de prueba de los mensajes y comunicaciones electrónicas que han sido remitidos al abogado por la parte contraria o el abogado de ésta, proporcionándole cierta información relevante para el proceso, por ejemplo, a efectos de intentar algún acuerdo. Nada impide que tales comunicaciones se aporten al proceso por cualquiera de los intervinientes en las mismas, salvo que estén protegidas por un deber de confidencialidad (por ejemplo, la que se puede derivar de haberse intentado previamente una mediación). Con todo, ello no obsta para que el abogado que así

20. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 229.

21. *Vid.*, AAP de Pontevedra 893/2017, de 25 de octubre (JUR 2017, 308428).

actúa pueda incurrir en algún tipo de responsabilidad disciplinaria por incumplir las normas deontológicas relativas a las comunicaciones entre letrados[22].

III. APORTACIÓN AL PROCESO DE LA FUENTE DE PRUEBA: MEDIO DE PRUEBA

Las fuentes de prueba electrónicas o digitales (mensajes o comunicaciones electrónicas) obtenidas lícitamente por las partes pueden introducirse o aportarse al proceso de distintas formas, aunque, *a priori*, ninguna de ellas garantiza absolutamente la autenticidad e integridad del mensaje o comunicación, porque tanto la autoría como el contenido del mismo son susceptibles de manipulación o alteración. Por tanto, como veremos, la validez y suficiencia probatoria de estas fuentes de prueba dependerá en buena medida del cauce procesal o medio de prueba a través del cual se introduzcan en el proceso y de la actitud que adopte respecto de ellas la parte contraria a la que perjudique la prueba, es decir, según admita su validez o impugne su autoría o autenticidad. Esta impugnación abrirá la posibilidad, según el criterio judicial, de que la parte que aportó las pruebas digitales impugnadas desarrolle una actividad probatoria complementaria para tratar de acreditar la validez, autenticidad e integridad de las comunicaciones electrónicas aportadas, por ejemplo, mediante una prueba pericial informática.

Pero esto es una cuestión que afecta al valor probatorio del medio de prueba, que luego veremos, no a lo que ahora interesa que son las formas admisibles de introducir en el proceso estas fuentes de prueba; o dicho de otro modo, ¿cuáles son los medios de prueba a través de los cuales se pueden introducir en el proceso estas fuentes de prueba digitales?[23].

A falta de una previsión legal sobre específicos medios de prueba para introducir en el proceso estas nuevas fuentes electrónicas o digitales, tendremos que echar mano de los medios de prueba tradicionales que mejor se adecúen a la naturaleza y características de esta fuentes[24], siendo

22. *Vid.*, RICHARD GONZÁLEZ, M., "Valor como prueba de los mensajes y comunicaciones electrónicas…", *op. cit.*, p. 231.
23. A este respecto, MAGRO SERVET ("¿Cómo aportar la prueba digital…?", *op. cit.*, pp. 3 a 8) reflexiona sobre la problemática que conlleva la falta de autonomía de la prueba digital, respecto de los medios de prueba tradicionales, es decir, la necesidad de canalizar la introducción en el proceso de estas nuevas fuentes de prueba a través de los cauces o medios de prueba tradicionales, previstos legalmente.
24. *Vid.*, MAGRO SERVET, V., "¿Cómo aportar la prueba digital…?", *op. cit.*, pp. 5-8. En el mismo sentido, ARRABAL PLATERO, P., "La prueba documental como medio para

recomendable la utilización de varios de estos medios de forma cumulativa para afianzar su valor probatorio[25]. Así, aunque se podrá utilizar otros, los más habituales serán los siguientes: la prueba de reconocimiento judicial (arts. 299.2 y 382 y 384 LEC), la prueba documental y la prueba testifical (o interrogatorio del acusado).

1. LA PRUEBA DE RECONOCIMIENTO JUDICIAL: REPRODUCCIÓN Y VISIONADO DE WEBS Y MENSAJES (TEXTO, IMAGEN, AUDIO O VIDEO) APORTADOS EN FORMATO ELECTRÓNICO

Puesto que se trata de fuentes de prueba en formato electrónico, (mensajes y comunicaciones electrónicas, contenidos de webs o redes sociales) lo normal, aunque no lo habitual, sería aportarlos al proceso en ese mismo formato, al amparo de los arts. 299.2, 382 y 384 LEC, para que puedan ser objeto de un reconocimiento judicial por el órgano enjuiciador.

Esta forma de aportación sería particularmente indicada cuando se pretende incorporar como prueba el contenido de páginas web o redes sociales. En tal caso, al proponer la prueba en el correspondiente escrito de calificación provisional, se debe indicar la web o red social que se ha de visionar en el juicio, y solicitar que ese día estén disponibles en la sala de vistas los medios técnicos necesarios para poder realizar esta reproducción y visionado (u ofrecerse la parte proponente a aportarlos).

Pero, dado el carácter volátil de estas fuentes de prueba, esta forma de aportación comporta el riesgo de que el contenido que se pretende visionar en el juicio sea retirado por la parte contraria con anterioridad al día del juicio. Por ello, es conveniente proceder al "aseguramiento de la prueba digital", y una forma de hacerlo sería aportándola también

aportar evidencias tecnológicas", *Elderecho.com*, https://elderecho.com/la-prueba-documental-como-medio-para-aportar-evidencias-tecnologicas, última consulta: 07/06/2022; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 2 y 3; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías", *Revista General de Derecho Procesal*, 44 (2018), p. 19; GÓMEZ CONESA, A., "El papel de WhatsApp y redes sociales en el proceso penal del Siglo XXI (1)", *Diario La Ley*, n.º 9858, Sección Tribuna, 26 de mayo de 2021, (La Ley 5309/2021), pp. 8 y 9.

25. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer cometidos a través de las nuevas tecnologías", *Revista Acta Judicial*, núm. 7, enero-junio 2021, p. 24; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 3; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 19.

de modo documental, por ejemplo, mediante un acta notarial, en la que se deje constancia del contenido que el notario pudo visionar en dicha página web o red social[26].

Además del contenido de páginas web y redes sociales, también podrán ser objeto de este reconocimiento judicial los mensajes y comunicaciones electrónicas (por ejemplo, los mensajes de Whatsapp o de correo electrónico con archivos de imagen, audio o vídeo). A tal efecto, se puede aportar y consignar ante el letrado de la Administración de Justicia, a fin de garantizar la cadena de custodia, el propio dispositivo en el que se recibió el mensaje (teléfono móvil, tablet, …), el disco duro del ordenador, o una memoria USB o tarjeta de memoria en la que se hayan almacenado los mensajes, y pedir que sean visionados en el juicio oral o examinados por el tribunal (art. 384.1 LEC).

A estos efectos, tratándose de mensajes de Whatsapp, se vería reforzado su valor probatorio si se aportasen los dos terminales o dispositivos implicados en la comunicación (el de emisión y el de recepción), porque, dadas las características técnicas de esta aplicación de mensajería, ello permitiría el reconocimiento y cotejo de los mismos por el juez, a efectos de acreditar el contenido de los mensajes y su presencia en los terminales de emisión y recepción[27].

En cualquier caso, será conveniente que, además de aportar los mensajes o correos en formato electrónico, también se acompañe la impresión o transcripción de los mismos (con o sin el apoyo de un informe pericial informático o acta notarial) para facilitarle al tribunal el acceso al contenido de esas comunicaciones electrónicas.

---

26. A tal efecto, matiza MAGRO SERVET ("¿Cómo aportar la prueba digital…?", *op. cit.*, p 8) que será suficiente aportar como documental el acta notarial, como prueba subsidiaria a la de reconocimiento judicial del contenido de la web o red social, sin que sea necesario proponer la testifical del notario que extendió el acta, porque no se requiere que el notario ratifique el acta en el juicio para que ésta haga prueba de su contenido.

27. En este sentido, señala CUAIRÁN ("La aportación de WhatsApps como medio de prueba…", *op. cit.*, p. 4) que, si bien los mensajes de WhatsApp son perfectamente utilizables como medios de prueba en un proceso penal, debiendo estarse al principio de libre valoración de la prueba por parte del juez, la configuración técnica actual de este servicio de mensajería no permite garantizar sin lugar a duda razonable la autenticidad de las conversaciones ni la integridad de su contenido, si no es mediante el cotejo de todos los terminales intervinientes en la conversación. *Vid.*, asimismo, ARMENTA DEU, T., "Regulación legal y valoración probatoria de fuentes de prueba digital…", *op. cit.*, p. 73; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 7.

2. LA PRUEBA DOCUMENTAL: APORTACIÓN MEDIANTE LA TRANSCRIPCIÓN DEL MENSAJE O IMPRESIÓN DE LA CAPTURA DE PANTALLA

El medio de prueba más común para aportar al proceso las fuentes de prueba digitales, en particular cuando se trata de mensajes de texto o, incluso, de imagen y audio, es la prueba documental. Es decir, se pueden imprimir los mensajes de texto o la captura de pantalla en la que aparece el mensaje (el llamado "pantallazo"), o transcribir los mensajes de audio, y presentarlos en el Juzgado de Instrucción como prueba documental[28].

No obstante, a efectos de reforzar la solidez y valor de esta prueba, es decir, la confianza en su autenticidad e integridad, es conveniente tener en cuenta dos aspectos. En primer lugar, será conveniente que la impresión recoja toda la cadena de mensajes que se refieren al mismo hecho relevante que se pretende acreditar, pues ello permite al tribunal conocer y comprender mejor el contexto general de la comunicación en el que se remite el mensaje. Y, en segundo, tratándose de correos electrónicos, es conveniente que el "pantallazo" incluya la "cabecera del correo", pues en ella figuran datos relevantes para acreditar la autenticidad e integridad del correo, tales como el remitente, el destinatario, el asunto, la fecha y hora en que fue redactado, la fecha y hora en que fue recibido, los servidores por los que ha pasado, etc.

Esta impresión o transcripción que se aporta al proceso la puede hacer la propia parte privadamente, pero ello ofrecería pocas garantías sobre la autenticidad e integridad del mensaje documentado. Por ello, el valor probatorio de esta prueba documental se puede ver reforzado de tres modos, que permiten incrementar la confianza en la autenticidad e integridad de la comunicación electrónica[29].

---

28. En este sentido, afirma FUENTES SORIANO ("Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 24) que, se asume, como punto de partida, que la parte interesada podrá aportar al proceso como fuente de prueba de una comunicación determinada la mera captura de pantalla con la conversación, sin tener que dar, *a priori*, muestras de la autenticidad y originalidad del documento. Esta forma de aportación ha sido admitida, entre otras, por las SSTS 300/2015, de 19 de mayo (RJ 2015, 1920) y 754/2015, de 27 de noviembre (RJ 2015, 5552); 375/2018, de 19 de julio (RJ 2018, 3771); 332/2019, de 27 de junio (RJ 2019, 2792).

29. No obstante, la STSJ Galicia 556/2016, de 28 enero (JUR 2016, 45246), se muestra más exigente y declara que no basta con la aportación del pantallazo como documento privado, sino que es necesario aportar también su trascripción y exige fe pública sobre la concordancia entre ambos: "para considerar una conversación de WhatsApp como documento –a los fines del proceso laboral–, sería preciso que se hubiese aportado no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, "pantallazo" –que es lo único se cumple por el actor–, sino una transcripción de la conversación y la comprobación de que de que ésta se corresponde con el teléfono y

El primero consistiría en la aportación de los mensajes documentados mediante acta notarial, es decir, mediante la intervención del notario como fedatario público. Pero con tal intervención del notario tampoco se garantiza de modo indubitado la autenticidad e integridad de la comunicación, sino únicamente el hecho concreto del que da fe el notario, y que dependerá del tipo de intervención que se le pida.

Así, la intervención del notario puede consistir simplemente en protocolizar la impresión o transcripción del mensaje electrónico que le presenta la parte, de modo que solo da fe de la identidad del sujeto que solicita la protocolización, del contenido del documento entregado (la impresión o transcripción del mensaje) y la fecha en que lo recibe. Pero la intervención del notario también puede consistir en acceder directamente al mensaje almacenado en el terminal o dispositivo electrónico, y levantar un acta de su contenido. En tal caso, daría fe del contenido del mensaje y de que dicho mensaje se encuentra almacenado en ese dispositivo concreto; lo que, a su vez, permitirá acreditar que, a partir de ese momento, el mensaje no fue manipulado. Pero el notario no puede dar fe de la autenticidad e integridad del mensaje, porque pudo haber sido manipulado anteriormente[30]. Finalmente, el notario también puede actuar como depositario del terminal o dispositivo electrónico en el que se almacenan los mensajes, a efectos de su aportación posterior al proceso, lo que permitirá garantizar que, a partir de ese momento, no se produce ninguna manipulación del dispositivo ni de la autoría y contenido del mensaje.

En segundo lugar, esta función del notario también puede ser realizada por el LAJ, aunque no es frecuente que se presten a ello, si bien no existe ninguna norma que lo prohíba. Si se le presenta el terminal o dispositivo

---

con el número correspondientes. Esto podría haber conseguido a través de la aportación del propio móvil del Sr. Abel y solicitando que, dando fe pública, el LAJ levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y de que éste se corresponde con el teléfono y con el número correspondientes; o, incluso, mediante la aportación de un acta notarial sobre los mismos extremos". Y añade que: "Apurando nuestras consideraciones sobre la prueba de mensajería instantánea y con fines esclarecedores, para que aceptemos como documento una conversación o mensaje de este tipo (algo diferente a su valor probatorio) podríamos establecer cuatro supuestos: (a) cuando la parte interlocutora de la conversación no impugna la conversación; (b) cuando reconoce expresamente dicha conversación y su contenido; (c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición); o, finalmente, (d) cuando se practique una prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores".

30. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, p. 4; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 19; GÓMEZ CONESA, A., "El papel de WhatsApp y redes sociales…", *op. cit.*, p. 8.

en el que se almacenan los mensajes, junto con la impresión o transcripción de los mismos, el LAJ puede acceder al terminal, verificar la existencia y contenido de los mensajes y levantar un acta por la que da fe de que la impresión o transcripción aportada es fiel reflejo del contenido de los mensajes almacenados en el terminal, así como del modelo y número de dicho terminal. Con ello se daría fe del contenido de los mensajes y de que se recibieron en dicho dispositivo concreto.

Esta forma de aportación se ha admitido, entre otras, por la SAP de Córdoba 159/2014, de 2 de abril y por la SAP de Alicante 753/2015, 9 de diciembre[31]. En ellas, se afirma lo siguiente: "En la legislación procesal actual no existe regulación específica de la prueba electrónica pese a que, como canal de comunicación, actos jurídicos y hechos con trascendencias jurídica se producen cada vez en más ocasiones a través de WhatsApp (…). Si bien en la práctica, los juzgados y tribunales suelen admitir dichas pruebas e incorporarlas al procedimiento tras realizar un cotejo de las mismas. En el caso de los mensajes de WhatsApp, se requiere a la parte que los alega para que acuda al juzgado con el dispositivo móvil y se proceda, por parte del secretario judicial, a cotejar su contenido desde el propio dispositivo con las transcripciones aportadas en papel, levantando acta por la que se de fe de que dicha documental es fiel reflejo del contenido de la conversación guardada en el móvil, así como del modelo y número de teléfono del mismo".

Como se ha dicho, a través de estas formas de aportación que hemos visto se puede acreditar que un mensaje electrónico ha sido recibido en un determinado dispositivo o terminal, y cuál es el contenido del mismo. También se podría acreditar que, a partir de un determinado momento (por ejemplo, desde que se deposita el dispositivo ante el notario o el LAJ) tal comunicación no ha sido manipulada o alterada. Pero tales formas de aportación no permiten acreditar de modo indubitado la autenticidad (es decir, la autoría real) y la integridad (es decir, que su contenido original no fue manipulado o alterado antes de su aportación) del mensaje electrónico[32]. Tales extremos solo se pueden acreditar fehacientemente mediante un análisis pericial informático del dispositivo.

31. SAP de Córdoba 159/2014, de 2 de abril (JUR 2014, 168647) y en la SAP de Alicante 753/2015, 9 de diciembre (JUR 2016, 132447).

32. Sobre los conceptos de autenticidad e integridad, *Vid.*, arts. 8 y 10 del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación: la autenticidad del origen de una factura garantiza la identidad del obligado a su expedición y del emisor de la factura; y la integridad del contenido garantiza que el mismo no ha sido modificado. *Vid.*, DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 5.

Ahora bien, tal informe pericial informático no es necesario siempre que se trate de aportar al proceso una fuente de prueba de carácter electrónico. Solo será necesario, en su caso, si la parte adversa impugna, cuestiona la autenticidad o integridad del mensaje. Si no las cuestiona, o incluso admite expresamente dicha comunicación y su contenido, bastará la aportación como prueba documental de la impresión o transcripción del mensaje para probar su realidad y contenido.

3. LA PRUEBA TESTIFICAL: APORTACIÓN MEDIANTE LA DECLARACIÓN TESTIFICAL DE TERCEROS QUE HAYAN VISTO EL MENSAJE EN EL DISPOSITIVO

Finalmente, las fuentes de prueba electrónicas o digitales también se pueden introducir en el proceso a través de la prueba testifical (o interrogatorio del acusado). Es decir, la existencia y contenido del mensaje o comunicación electrónica en cuestión también se puede introducir en el proceso a través de la declaración testifical de personas que hayan visto dicho mensaje y su contenido en el dispositivo o terminal de envío o recepción (o mediante el interrogatorio del acusado sobre el envío de tal mensaje).

IV. IMPUGNACIÓN Y VALOR PROBATORIO

Al igual que para las demás pruebas en el proceso penal, para la valoración probatoria de estas fuentes de prueba electrónicas o digitales rige el principio de libre valoración de la prueba, es decir, el juez debe valorarlas conforme a las reglas de la sana crítica y según las máximas de experiencia (así resulta de los arts. 382.3 y 384.3 LEC, que son de aplicación subsidiaria a todas las jurisdicciones, y del art. 741 LECrim), y teniendo en cuenta las demás pruebas practicadas (valoración conjunta de la prueba)[33].

33. *Vid.*, DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 4, 6 y 7. Señala este autor que la libre valoración de la prueba electrónica, "en primer lugar, quiere decir que la Ley no obliga al Juez a tener por probados los hechos que surjan de una prueba electrónica; salvo los supuestos de documento público electrónico. En segundo lugar, significa que la Ley no determina que la prueba electrónica solamente puede tener eficacia probatoria si se cumplen ciertos presupuestos legales; sino que cualquier prueba electrónica puede, en principio, desplegar efectos para acreditar un hecho relevante para el proceso. Otra cosa es la verosimilitud o eficacia probatoria que el Juez otorgue a una concreta prueba digital de conformidad con las reglas de la sana crítica. En tercer lugar, también quiere decir que el Juez valorará la prueba electrónica conforme a las reglas de sana crítica según la naturaleza del soporte en que se hayan aportado los datos; en definitiva, una valoración conforme a las reglas

Esto significa que el valor probatorio que pueden alcanzar estas fuentes de prueba dependerá de varios factores[34]: a) la propia tecnología de comunicación utilizada y, en particular, la facilidad de manipulación de la misma; b) el medio de prueba a través del cual se ha introducido en el proceso, lo que, a su vez determina la solidez de la autenticidad e integridad de la fuente de prueba (por ejemplo, si se ha aportado la simple impresión de la captura de pantalla o se aportó acta notarial con la transcripción del mensaje); y, c) fundamentalmente, dependerá de la actitud procesal de la parte a la que perjudica esta prueba, es decir, de si impugna o no la autenticidad e integridad de la comunicación.

1. LA PARTE CONTRARIA NO IMPUGNA LA AUTENTICIDAD Y/O INTEGRIDAD DE LA FUENTE DE PRUEBA

Si, ante la aportación de la fuente de prueba electrónica o digital en cualquiera de las modalidades que hemos visto (incluso una simple impresión de un pantallazo), la parte contraria a la que perjudica no impugna su autenticidad y/o integridad, ésta podría alcanzar pleno valor probatorio, y, en base a ella, el juez podría dar por probada la existencia, autoría y contenido de la comunicación electrónica en cuestión. Y ello, sin necesidad de ninguna prueba adicional sobre su autenticidad o integridad. Además, a estos efectos, por no impugnación cabe entender tanto la ratificación o reconocimiento expreso de la existencia y contenido de la comunicación por parte de los interlocutores, como el silencio de la parte a la que perjudica la prueba[35].

Que alcance o no este valor probatorio pleno dependerá de la aplicación que haga el juez del criterio de la libre valoración de la prueba, que

---

de criterio racional, es decir, de forma ajustada a las reglas de la lógica, los principios de la experiencia y los conocimientos científicos. En cuarto lugar, el alto componente tecnológico de la prueba electrónica determinará con frecuencia la importancia de los conocimientos científicos en su valoración, por lo que la prueba pericial tiene una especial relevancia en este ámbito. En quinto lugar, en la valoración conforme a la sana crítica el Juez habrá de tener en cuenta la postura procesal de cada una de las partes en relación con la concreta prueba electrónica: especialmente, si ha existido impugnación por la parte no proponente y el fundamento de dicha impugnación" En el mismo sentido, FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias…*, *op. cit.*, p. 8.

34. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, p. 26; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 3 y 4; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 20.

35. *Vid.*, STS 469/2017, de 22 de junio (RJ 2017, 3569); SAP de Córdoba 159/2014, de 2 de abril (JUR 2014, 168647); o SAP de Teruel 23/2017, de 21 de junio (ARP 2017, 1057).

deberá motivar en la sentencia. Y, como dijimos, a tal efecto será determinante la facilidad de manipulación del tipo de tecnología de comunicación utilizada, la confianza sobre la autenticidad e integridad que proporcione el concreto medio de prueba utilizado, así como el resto de las pruebas válidamente practicadas en el proceso.

Este valor probatorio responde a la máxima de experiencia conforme a la cual, si la parte a la que perjudica la prueba no impugna la autenticidad o integridad de la comunicación, el juez puede tenerla por cierta y acreditada; y ello, aunque en la realidad pueda haber sido falseada. Pero, si la parte a la que perjudica la prueba no la impugna, no existe razón alguna que justifique gravar a la parte que la aporta con la carga de tener que aportar un informe pericial informático u otra prueba adicional sobre la autenticidad e integridad de la comunicación que nadie ha cuestionado[36].

2. LA PARTE CONTRARIA IMPUGNA LA AUTENTICIDAD Y/O INTEGRIDAD DE LA FUENTE DE PRUEBA

Si la parte contraria, a la que perjudica la prueba electrónica o digital, la impugna[37], poniendo en cuestión su autenticidad y/o integridad, no por ello pierde automáticamente todo su valor probatorio, porque continúa rigiendo el principio de libre valoración de la prueba. Por tanto, pese a la impugnación, a partir de la valoración conjunta de toda la prueba aportada, y de todas las circunstancias concurrentes, el tribunal puede dar por probada igualmente la existencia, autoría y contenido de la comunicación.

Es decir, la impugnación de la prueba no conlleva la sustitución automática del principio de libre valoración de la prueba por una distribución formal de la carga de la prueba, en el sentido de que se produzca una "inversión de la carga de la prueba", de modo que, si la parte a la que beneficia la prueba no consigue acreditar fehacientemente su autenticidad e integridad, el juez no pueda tenerla por válida. No, sigue rigiendo el principio de libre valoración de la prueba, conforme a las reglas de la sana crítica y las máximas de experiencia. Pero, precisamente por eso, las alegaciones impugnatorias con suficiente seriedad por la parte adversa

36. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, p. 26; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 20; GONZÁLEZ LAGE, J., "La prueba pericial en la práctica judicial penal: las redes sociales en el proceso penal", en *Peritaje y prueba pericial* (Dir., Picó i Junoy, J.), Bosch, Barcelona, 2017, p. 565. *Vid.*, asimismo, STS 300/2015, de 19 de mayo (RJ 2015, 1920).

37. Sobre el momento y forma de impugnar la prueba electrónica o digital, *Vid.*, MAGRO SERVET, V., "¿Cómo aportar la prueba digital…?", *op. cit.*, p. 5.

de la validez de esta prueba, puede determinar la necesidad de reforzarla con otra actividad complementaria tendente a acreditar o afianzar la existencia, autenticidad e integridad de la comunicación. Es decir, a la parte a la que favorezca la prueba ya no le basta con aportarla por alguno de los medios que hemos visto, sino que deberá aportar prueba complementaria sobre la autenticidad e integridad de la comunicación[38].

Pero, a este respecto, se plantean dos cuestiones importantes. La primera es, ¿cómo debe ser la impugnación?; es decir, ¿basta con negar la autenticidad o integridad de la comunicación o debe estar fundamentada tal impugnación? Y, la segunda, ante tal impugnación, ¿qué medios se pueden utilizar para tratar de acreditar la autenticidad e integridad cuestionada?

Por lo que se refiere al primer interrogante, cabe destacar que no cualquier impugnación de la autenticidad e integridad de la fuente de prueba electrónica va a determinar la necesidad de una actividad probatoria complementaria para acreditar tales extremos. Ha de tratarse de una impugnación con suficiente seriedad. Y, a los efectos de valorar la seriedad de tal impugnación, deben tenerse en cuenta, al menos, dos elementos[39].

En primer lugar, se deberá atender al contenido y fundamento de la impugnación, es decir, tal impugnación ha de tener un respaldo alegatorio, ha de estar fundada en argumentos e indicios serios, claros y exhaustivos, que permitan poner en duda la autenticidad e integridad de la comunicación[40]. Así, por ejemplo, la SAP de Vizcaya 90308/2014, de 24 de julio, considera insuficiente a estos efectos la mera alegación genérica de que "el WhatsApp es fácilmente manipulable"[41].

38. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 30 y 31; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, pp. 5 y 6; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 25.

39. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 31 y 32; DELGADO MARTÍN, J., "La prueba del Whatsapp…", *op. cit.*, p. 6.; GONZÁLEZ LAGE, J., "La prueba pericial en la práctica judicial penal…", *op. cit.*, pp. 565 y 566.

40. Como señala ARRABAL PLATERO ("La prueba documental…", *op. cit.*,), si bien la jurisprudencia no pide un "principio de prueba" a la parte impugnante, sí le pide que introduzca elementos de duda sobre la autenticidad e integridad de la prueba aportada de opuesto que se adicionen al acervo probatorio y contribuyan a desacreditar la prueba impugnada, descartando las tesis impugnatorias que resultan del todo rocambolescas y ausentes de más justificación que las únicas afirmaciones del impugnante.

41. Señala la SAP de Vizcaya 90308/2014, de 24 de julio (JUR 2014, 268182) que "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

Y, en segundo lugar, también se deberá valorar la diligencia de la parte que impugna la prueba a la hora de proponer otros medios probatorios que puedan poner en cuestión la autenticidad e integridad de la prueba digital. Por ejemplo, se podría cuestionar la autoría del mensaje, si se acredita que, en el momento del envío de tal mensaje, el teléfono estaba extraviado y no tenía contraseña de acceso, de modo que cualquier persona que lo tuviera en su poder podría haber enviado dicho mensaje.

En este sentido, la STS 300/2015, de 19 de mayo, desestimó la impugnación de la autenticidad de una conversación mantenida en Tuenti, formulada por la defensa, entre otros motivos, porque la acusación particular puso a disposición del Juzgado de Instrucción las claves personales de la víctima en Tuenti para que, si la conversación era cuestionada, se pudiese oficiar a Tuenti España para que se certificara el contenido de esa conversación, sin que la defensa hubiese hecho petición alguna al respecto[42].

A su vez, en cuanto a los medios que se pueden utilizar por la parte proponente para tratar de acreditar o corroborar la autenticidad e integridad de la comunicación electrónica impugnadas, ello dependerá de cuál haya sido el canal o medio tecnológico que se ha utilizado para dicha comunicación, pues a tal efecto resultan determinantes las específicas características técnicas de unos y otros.

2.1. En el caso de aplicaciones de mensajería instantánea (Whatsapp)

La aplicación de mensajería instantánea de Whatsapp presenta dos importantes vulnerabilidades que repercuten en la fiabilidad de sus mensajes como fuente de prueba y en el modo en que se puede tratar de acreditar la misma[43].

La primera es la facilidad con la que pueden ser manipulados los mensajes de Whatsapp, de modo que incluso existen aplicaciones que permiten crear conversaciones de Whatsapp ficticias (por ejemplo, Whatsapp

---

valoración probatoria en el sentido interesado en el recurso. Todo apunta a la autoría de la receptación por el acusado, ya que los objetos sustraídos 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".

42. *Vid.*, STS 300/2015, de 19 de mayo (RJ 2015, 1920).

43. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, p. 2 y 3.

Fake Chat). De ella se hacen eco, entre otras, las SSTS 300/2015, de 19 de mayo, 375/2018, de 19 de julio y 332/2019, de 27 de junio[44], señalando 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".

Y la segunda vulnerabilidad referida, radica en que las conversaciones de Whatsapp no quedan almacenadas en ningún servidor externo del proveedor del servicio, sino únicamente en los dispositivos de envío y recepción, por lo que no es posible solicitar copias de los mensajes ni certificación de sus contenidos al proveedor. El proveedor del servicio únicamente conserva una información limitada sobre datos de tráfico o los relativos a identificación de usuarios, número de abonado telefónico o identificación de direcciones IP. Por tanto, la única forma de acreditar indubitadamente la autenticidad e integridad de los mensajes de Whatsapp, es decir, su existencia, autoría y contenido original, será a través de un análisis pericial consistente en el cotejo de los terminales de envío y recepción. Pero, si los comunicantes eliminan los mensajes de sus terminales, será muy difícil la práctica de una pericia informática capaz de acreditar al cien por cien su autenticidad e integridad.

Pero, aun en este caso, cabría alguna posibilidad de corroborar la autenticidad e integridad de los mensajes en ciertos supuestos[45]. Ello es así porque la aplicación de Whatsapp permite al usuario usar servicios de almacenamiento en la nube (ICloud o Google Drive) para hacer copias de seguridad de los mensajes, que se suelen hacer automáticamente. En tal caso, se podría solicitar a estos proveedores copia de los mensajes guardados y cotejarlos con las evidencias aportadas al proceso. Pero lo que no se podría es acreditar que tales mensajes no han sido manipulados antes de hacerse la copia de seguridad. Además, en el caso de conversaciones

44. *Vid.*, SSTS 300/2015, de 19 de mayo (RJ 2015, 1920); 375/2018, de 19 de julio (RJ 2018, 3771); y 332/2019, de 27 de junio (RJ 2019, 2792).

45. *Vid.*, CUAIRÁN, J., "La aportación de WhatsApp como medio de prueba…", *op. cit.*, pp. 3 y 4; FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit.*, pp. 9 y 10.

mantenidas a través de un grupo de Whatsapp, todos los usuarios del grupo han recibido el mensaje, por lo que la aportación de una copia de esta conversación, junto con la declaración testifical de varios miembros del grupo sería de gran relevancia para acreditar la autenticidad e integridad de la comunicación.

Con todo, la imposibilidad de esta prueba pericial, no implica que estos mensajes pierdan todo su valor probatorio en caso de impugnación. Es decir, la prueba pericial informática no es el único e indispensable medio de dotar de valor probatorio al mensaje de Whatsapp, porque continúa rigiendo el principio de libre valoración de la prueba, por lo que el convencimiento del juez sobre la autenticidad e integridad de los mensajes puede apoyarse en otros elementos probatorios, como la declaración de testigos, o las manifestaciones de las partes[46].

2.2. En el caso de plataformas de redes sociales (Facebook, Instagram…)

Las plataformas de redes sociales presentan otras características y vulnerabilidades a efectos de su utilización como fuente de prueba distintas a las de las aplicaciones de mensajería instantánea, lo que determina que su tratamiento sea distinto a estos efectos.

En principio, por sus propias características, no plantea excesiva dificultad corroborar la integridad de la comunicación difundida a través de estas plataformas, es decir, el contenido de la comunicación, porque, aunque los usuarios pueden establecer distintos niveles de privacidad, en principio están destinadas a la difusión pública de los contenidos, por lo que, si se impugna la integridad de la comunicación, ésta se puede corroborar a partir de la información facilitada por cualquier de los usuarios que hayan tenido acceso al mismo.

Además, la información publicada a través de estas redes sociales suele conservarse en los servidores de los operadores de las mismas (durante aproximadamente 90 días), aunque el perfil correspondiente se haya eliminado, por si el usuario desea activarlo de nuevo. Por ello, se podrá obtener de los mismos, con autorización judicial, la información conservada cuando sea necesario verificar la integridad de las fuentes de prueba o evidencias aportadas por las partes al proceso. Y, a estos efectos, la propia policía podrá ordenar al operador la conservación de la información

46. *Vid.*, BUENO BENEDÍ, M., "La prueba en los procedimientos de violencia sobre la mujer…", *op. cit.*, pp. 30 y 31; FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 24 y 25.

almacenada en sus servidores hasta obtener la autorización judicial para la cesión de la misma (art. 588 octies LECrim)[47].

Más complejo puede ser verificar la autoría o autenticidad de la comunicación difundida. Como es sabido, para acceder y operar a través de estas plataformas y redes es necesario crear una cuenta de dominio, un perfil, con nombre de usuario y contraseña; y, frecuentemente, sobre todo para delinquir, se utilizan identidades falsas o seudónimos.

Pero, al utilizar estas plataformas, con cada acto de comunicación, se generan unos datos de tráfico y localización que quedan almacenados y que los operadores de servicios de comunicaciones electrónicas deben conservar (normalmente, durante 12 meses desde la fecha de la comunicación) y, en su caso, ceder con fines de investigación y enjuiciamiento penal, conforme a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[48]. Por tanto, a partir de estos datos, se puede hacer un rastreo que permita identificar al verdadero autor de la comunicación[49].

Este rastreo se puede hacer a partir de los datos almacenados y cedidos por parte de los operadores de servicios de comunicación, para lo cual será necesario contar con la correspondiente autorización judicial (arts. 1 y 7 Ley 25/2007 y 588 ter j) LECrim). Y hasta que se obtenga tal autorización, el MF o la policía podrán ordenar la conservación y protección de tales datos (art. 588 octies LECrim)[50].

---

47. *Vid*., FISCALÍA GNERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit*., pp. 11 y 12.

48. Los datos que los operadores deben conservar son los previstos en el art. 3 Ley 25/2007: a) datos para rastrear e identificar el origen de la comunicación (identificación de usuario y número de teléfono asignados); b) datos para identificar el destino de la comunicación; c) datos para determinar la fecha, hora y duración de la comunicación; d) datos para identificar el tipo de comunicación (servicio de internet utilizado); e) datos para identificar el equipo de comunicación; o, f) datos necesarios para identificar la localización del equipo de comunicación.

49. *Vid*., FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 30 a 32.

50. A este respecto, es necesario recordar que la Ley 25/2007, de 18 de octubre, se aprobó con objeto de transponer la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, que fue declara inválida por la sentencia del TJUE (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland*, C-293/12, sobre la base de que el Derecho de la Unión Europea se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización relativos a las comunicaciones electrónicas con fines de lucha contra la delincuencia grave. Si bien la referida Ley no se ve anulada como efecto directo de esta sentencia, pues no está así previsto en el Derecho Comunitario, no puede obviarse la repercusión que la misma puede tener en los procedimientos judiciales en los que se haga uso de esta conservación y cesión de datos

Pero también se puede hacer a partir de otros datos que puede recabar directamente la policía, sin necesidad de autorización judicial, conforme a los arts. 588 ter k) a m) LECrim: a) acceso por la policía a una dirección IP (y luego solicitar autorización judicial para la cesión por el proveedor de servicios de los datos que permitan la identificación y localización del equipo y la identificación del usuario); b) captación por la policía de números IMSI o IMEI o de cualquier otro dato que identifique un equipo de comunicación o la tarjeta de acceso a la red de comunicaciones (y luego pedir autorización judicial para intervenir las comunicaciones); y, c) solicitar de los prestadores de servicios de comunicaciones la identificación del titular de un número de teléfono o el número de teléfono de un determinado titular o los datos identificativos de cualquier medio de comunicación[51].

Finalmente, si no fuese posible la corroboración de la autenticidad de la fuente de prueba impugnada a través de los medios tecnológicos señalados, todavía sería posible acreditarla por otras vías. Por ejemplo, si las partes o testigos admiten o declaran que el seudónimo utilizado en la comunicación es el que utiliza habitualmente el acusado; o si los testigos declaran que el acusado había anunciado su intención de comunicarse por esta vía con la víctima. Por tanto, como señala FUENTES SORIANO, aun cuando la autenticidad de la comunicación aportada como fuente de prueba no se hubiese podido acreditar en virtud de una investigación tecnológica, sería posible otorgar valor probatorio, más o menos contundente, a esa comunicación a partir del acervo probatorio existente en el caso concreto. Ahora bien, dada la relativa facilidad con que puede adverarse la información transmitida a través de estas plataformas de redes sociales (a diferencia de lo que sucede con las aplicaciones de mensajería instantánea), el valor probatorio que pueda alcanzar dicha comunicación a partir de otros posibles medios de prueba practicados debería ser totalmente fiable e incuestionado, y reflejarse así en la fundamentación de la sentencia[52].

No obstante, estas formas de corroborar la autenticidad de la comunicación aportada como fuente de prueba plantean en la práctica dos problemas.

---

reguladas por esta Ley. Por tanto, deberán ser los jueces y tribunales españoles los que valoren caso por caso la aplicación de la Ley 25/2007, de 18 de octubre, tratando de ajustarse al principio de proporcionalidad en los términos fijados en la referida sentencia del TJUE.

51. *Vid.*, LARO GONZÁLEZ, M.ª E., "Prueba electrónica: situación actual en el proceso penal y perspectivas de futuro", en (Dir., Conde Fuentes, J. y Serrano Hoyo, G.), *La justicia digital en España y en la Unión Europea*, Atelier, Barcelona, 2019, p. 248.
52. FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, p. 32.

En primer lugar, conforme al art. 1 Ley 25/2007, la obligación de los operadores de servicios de comunicaciones electrónicas de conservar y ceder los datos de tráfico que se generan y tratan se limita a la investigación y enjuiciamiento de "delitos graves", por lo que quedarían fuera de su ámbito un buen número de delitos cometidos constitutivos de esta violencia de género digital, que no tienen la consideración de graves conforme a los arts. 13 y 33 CP.

No obstante, a este respecto, a raíz del AAP de Madrid 131/2015, de 25 de febrero[53], se va consolidando la tesis de que, a estos efectos, la "gravedad" del delito no puede medirse exclusivamente atendiendo a su "penalidad"; sino que, habrá que tener en cuenta también otros criterios tales como la importancia y relevancia social del bien jurídico protegido, la trascendencia social de los efectos del delito o su comisión por organizaciones criminales. Por tanto, a la vista de estas circunstancias, se podrían utilizar estos medios de investigación aun tratándose de delitos que, por su penalidad, tengan la consideración de "menos graves"[54].

El segundo problema apuntado se refiere a que la mayoría de estos proveedores de servicios de comunicaciones electrónicas tienen su sede fuera de nuestro país, generalmente en EEUU, lo que obligará a acudir a solicitudes de auxilio judicial internacional[55]. A estos efectos, será importante la próxima aprobación del Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[56], y de la Directiva

53. AAP de Madrid 131/2015, de 25 de febrero (JUR 2015, 66473). Declara este Auto que "entendemos que los "delitos graves" a que se refiere la Ley 25/2007 no son exclusivamente los delitos castigados con pena superior a cinco años, sino que también han de incluirse en tal expresión aquellos otros delitos castigados con pena inferior y que, por tanto, tienen la calificación legal de "delitos menos graves", pero que merezcan la consideración de graves en atención a otros parámetros, tales como la importancia del bien jurídico protegido, la trascendencia social de los efectos que el delito genera o la inexistencia de medios alternativos, menos gravosos, que permitan su investigación y esclarecimiento. En este punto no puede desconocerse que los efectos socialmente nocivos de determinados hechos delictivos pueden verse incrementados exponencialmente desde el momento en que se alcanza la convicción social de su impunidad, con el consiguiente fracaso de los fines preventivos que su tipificación penal persigue".
54. FUENTES SORIANO, O., "Los procesos por violencia de género. Problemas probatorios…", *op. cit.*, pp. 27 y 28.
55. *Vid.*, FISCALÍA GENERAL DEL ESTADO, *Dictamen n.º 1/2016 sobre la valoración de las evidencias en soporte papel…*, *op. cit.*, p. 12.
56. *Vid., Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal* (COM(2018) 225 final) (https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0006.02/DOC_1&format=PDF).

del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales[57]. En ella, se contempla la obligación de los proveedores de servicios de comunicaciones electrónicas o de la sociedad de la información que presten sus servicios en la UE de designar un representante legal en la UE que será el responsable de recibir, cumplir y ejecutar las órdenes de entrega y conservación de esas pruebas penales electrónicas.

57. *Vid., Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales* (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0226&from=ES).