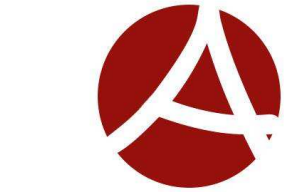

T R A B A J O F I N D E T Í T U L O

MÁSTER EN ACCESO A LA ABOGACÍA

Materia: Orden Jurisdiccional Penal

Curso 2015/2017

ESTUDIO DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL: ESPECIAL REFERENCIA A LAS CONVERSACIONES DE *WHATSAPP*

José Sánchez Hernández

Dirigido por Dra. Dª. Marta del Pozo Pérez

Diciembre 2016

T R A B A J O F I N D E T Í T U L O

MÁSTER EN ACCESO A LA ABOGACÍA

Materia: Orden Jurisdiccional Penal

Curso 2015/2017

Diciembre 2016

ESTUDIO DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL: ESPECIAL REFERENCIA A LAS CONVERSACIONES DE *WHATSAPP*

STUDY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: SPECIAL REFERENCE TO *WHATSAPP* TALKS

José Sánchez Hernández **Dirigido por Dra. Dª Marta del Pozo Pérez**

E-mail: jose_jsh@usal.es

Fdo.: **Fdo.:**

José Sánchez Hernández **Dra. Dª Marta del Pozo Pérez**

R E S U M E N

El presente Trabajo tiene por objeto realizar un estudio tanto teórico como práctico de la inclusión en el proceso, concretamente en la fase probatoria, de nuevos instrumentos que se han encuadrado dentro de lo que se ha denominado «prueba electrónica», haciendo especial referencia a la aplicación *WhatsApp*. Teniendo en cuenta el nacimiento exponencial de las denominadas «Tecnologías de la Información y la Comunicación», se ha generalizado el uso de nuevos medios de comunicación, entre los cuales se sitúan las aplicaciones de mensajería instantánea. Por consiguiente y en líneas generales, se pretende analizar el recorrido de la prueba electrónica siguiendo el orden lógico del proceso, o sea, se pretende analizar la licitud en la obtención de la prueba electrónica, las distintas formas de proponer y aportar la misma al proceso penal, para después conocer los medios de valoración y posterior autenticidad que emplean los Tribunales de Justicia españoles. Para finalizar, se expondrán las conclusiones que se han alcanzado tras el estudio teórico-práctico de la prueba electrónica en el proceso penal, y se propondrá la adaptación/reforma de las leyes procesales para conseguir una Justicia 2.0 que otorgue mayor seguridad jurídica.

P A L A B R A S C L A V E

Prueba; Electrónica; WhatsApp; Teléfono; Mensajería; Justicia 2.0; Obtención; Aportación; Validez; Legalidad; Autenticidad; Vulnerabilidad; Proceso; Penal.

A B S T R A C T

This paper aims to make a theoretical and practical study about the inclusion in the process, in particular in the probationary stage, the new instruments are named «electronic evidence», especially *WhatsApp*. Knowing the exponential birth of so-called «Technologies of the Information and Communication», the use of new media has been increased, including messaging apps. In general, it´s analysed the logic way of the electronic evidence in the process, that is, it´s analysed the lawfulness in the obtaining of the electronic evidence, the different way to pose and to provide the same in the penal process to know the valuation and authenticity that Spanish Courts of Justice use. To finish, the conclusions present, after the theoretical and practical study of the electronic evidence in the penal process, the change of the processual law to get a Justice 2.0 with more legal security.

K E Y W O R D S

Evidence; Electronic; WhatsApp; Messaging; Justice 2.0; Obtaining; Contribution; Validity; Legality; Authenticity; Insecurity; Process; Penal.

«Nada se parece tanto a la injusticia como la justicia tardía»

Séneca (4 a.C. – 65 d.C).

A los que me acompañan en el camino.

Gracias por estar ahí.

– ÍNDICE –

I. INTRODUCCIÓN: *NUEVOS TIEMPOS, NUEVAS PRUEBAS* 3

II. CONCEPTO, NATURALEZA, MARCO LEGAL, OBTENCIÓN Y LICITUD DE LA PRUEBA ELECTRÓNICA 6

1. *Aproximación al concepto de prueba electrónica* 6

2. *Sobre la naturaleza de la prueba electrónica: ¿equivalente a la documental?* 8

3. *Marco legal aplicable*: *de la ausencia de normativa específica* 12

3.1. Normativa estatal 12

3.2. Normativa comunitaria 16

3.3. Normativa internacional 16

4. *Obtención de la mensajería instantánea como medio de prueba: el juicio de licitud* 17

III. DE LA APORTACIÓN DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL 22

1. *Relevancia de la prueba electrónica en el orden jurisdiccional penal* 22

2. *Momento de proposición y aportación de la prueba electrónica en el proceso penal* 24

3. *De las formas de proposición y aportación de la prueba electrónica y su eficacia: del «pantallazo» al uso del «hash»* 27

IV. ADMISIÓN, PRÁCTICA Y VALORACIÓN DE LA PRUEBA ELECTRÓNICA EN EL ORDEN JURISDICCIONAL PENAL 33

1. *Admisión y práctica de la prueba electrónica* 33

2. *¿WhatsApp, prueba válida?: Análisis de los últimos pronunciamientos judiciales* 35

V. DE LA AUTENTICIDAD Y COTEJO DE LA PRUEBA ELECTRÓNICA 47

1. *La vulnerabilidad de las aplicaciones de mensajería instantánea: su fácil manipulación* 47

2. *Formas de autenticación: la necesaria práctica de prueba pericial informática* 49

3. *Protocolos para la autenticación: especial referencia a la norma ISO/IEC 27037:2012* 55

VI. CONCLUSIONES: **HACIA UNA *JUSTICIA 2.0*** 57

VII. RESEÑA BIBLIOGRÁFICA 61

I. INTRODUCCIÓN: *NUEVOS TIEMPOS, NUEVAS PRUEBAS*

El presente Trabajo Fin de Título tiene por objeto realizar un estudio, tanto teórico como práctico, de la inclusión en el proceso, concretamente en la fase probatoria, de nuevos instrumentos que se han encuadrado dentro de lo que se ha denominado «prueba electrónica». Como es sabido, la evolución de la Tecnología ha puesto en jaque el principio de adaptación del Derecho frente a los cambios sociales; y es que esa capacidad de ajuste del Derecho no puede neutralizar el aumento de ciertos escenarios que se generan a diario en nuestra Sociedad, y que derivan en cierto modo del nacimiento exponencial de las llamadas «Tecnologías de la Información y la Comunicación» (a partir de ahora, T.I.C.S.). Esto es, la Sociedad, ahora ya globalizada, ha cambiado, provocando que la forma de comunicación haya dado un giro de 180º.

Así pues, los nuevos medios de comunicación (*e-mails*, SMS, *Skype*, *YouTube*, *Facebook*, *Twitter*, *Instagram*, etc.) y, entre otras, las aplicaciones de mensajería instantánea (*WhatsApp*, *Allo*, *Line*, *Telegram*, *Hangouts*, *WeChat*, *BlackBerry Messenger*, *Facebook Messenger*, *Viber*, *Spotbros*, etc.) han adquirido especial relevancia en nuestras vidas, hasta el punto de que su uso se ha generalizado y se han convertido en auténticos instrumentos probatorios que se pretenden utilizar en vía judicial.

El hándicap de encontrarnos ante un escenario antes jamás vivido se agrava cuando nuestro Ordenamiento jurídico no es capaz de dar una respuesta válida, eficaz y real a situaciones que hasta ahora no existían. Lo que genera esto es una gran inseguridad jurídica e importantes situaciones de perjuicio para los intervinientes en los procesos judiciales, cuestiones que se dilatarán de no ser reguladas de forma específica y completa; en otras palabras, nos encontramos ante la ausencia de una regulación procesal concreta para este tipo de medio probatorio que, unido al riesgo evidente de manipulación de las conversaciones mantenidas en las distintas aplicaciones de mensajería instantánea, hace más que necesario incluir en la legislación española –y quizá en la comunitaria– métodos que otorguen autenticidad e integridad a esas conversaciones que se quieren proponer y aportar en un proceso judicial determinado.

Ahora bien, como la prueba electrónica es una materia excesivamente extensa, nos centraremos en el análisis de las conversaciones mantenidas a través de la aplicación *WhatsApp*. El motivo no es otro que su éxito, pues esta *app* de mensajería instantánea ha alcanzado a inicios del año 2016 (superando una vez más propio récord) los 1000 millones de usuarios mensuales en activo; cifras que solo unos pocos, como *Gmail*, *YouTube* o *Facebook*, son capaces de igualar[1]. Esto viene a equivaler a que una de cada siete personas en el mundo usa *WhatsApp*; es más, se calcula que el 70% de esos usuarios utilizan esta *app* a diario. Y, por si fuera poco, España se sitúa como el cuarto país del mundo –y a la cabeza de Europa– en el uso de esta aplicación de mensajería instantánea, alcanzando una cuota de penetración del 70% entre los usuarios de

[1] Datos obtenidos de «WhatsApp hace historia: supera los 1.000 millones de usuarios activos al mes», Diario *elEconomista.es*, 2 de febrero de 2016 [consultado 6 de noviembre de 2016].

telefonía móvil (por detrás de Sudáfrica –78%–, Singapur, –72%–, y Hong Kong, –71%–)[2].

Estos datos revelan un uso desmesurado de los teléfonos inteligentes, sus aplicaciones y redes sociales por parte de los españoles; tanto es así que, según datos de febrero de 2016, en *WhatsApp* se comparten cada día 42 billones de mensajes, 1,6 billones de fotos y 250 millones de vídeos[3]. Estos estratosféricos datos dejan en evidencia las deficiencias que sufre actualmente nuestra legislación, y más todavía en lo que se refiere al proceso penal. En este sentido, la aparición de las T.I.C.S. ha provocado la proliferación de los denominados «delitos informáticos» o «ciberdelitos» (entendidos como aquellas acciones antijurídicas y culpables que se dan por vías informáticas, o que tienen como objetivo principal destruir y dañar ordenadores, medios electrónicos o redes de Internet[4]).

Pues bien, los ciberdelitos, tales como las estafas de *phishing*[5], el *cyberstalking*[6], el *ciberbullying*[7], el *sexting*[8] o *child grooming*[9], han crecido en nuestro país a un ritmo veloz; y ese crecimiento fugaz ha provocado que, unido a que son realmente difíciles de

[2] «España, el cuarto país en el mundo en el uso de WhatsApp», Diario *ABC*, 25 de febrero de 2015 [consultado 6 de noviembre de 2016].

[3] «Las «aplastantes» cifras de WhatsApp: 2.000 millones de mensajes al día, 1.600 millones de fotos y 250 millones de vídeos», Diario *ABC*, 2 de febrero de 2016 [consultado 6 de noviembre de 2016].

[4] Definición creada a partir de: http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal

[5] La Sentencia número 69/2007 del Juzgado de Primera Instancia de Murcia, de 30 de marzo, define *phishing* como «un tipo de delito encuadrado dentro del ámbito de las estafas que se traduce en una táctica telemática mediante la cual el usuario es conducido a una página web con apariencia que es la de su entidad financiera y que se caracteriza por adquirir información confidencial de forma fraudulenta».

[6] Por *cyberstalking* se entiende aquella «conducta reiterada e intencionada de persecución obsesiva respecto de una persona, el objetivo, realizada en contra de su voluntad y que le crea aprensión o es susceptible de provocarle miedo razonable». Véase VILLACAMPA ESTIARTE, C.: *Stalking y Derecho Penal. Relevancia Jurídico-Penal de una Nueva Forma de Acoso*, Ed. Iustel, Madrid, 2009, pág. 57 y ss.

[7] El Auto número 291/2012 de la Audiencia Provincial de Cantabria (Sección 3ª), de 25 de mayo, hace una diferenciación entre acoso escolar y *ciberbullying*, pues entiende que el acoso escolar es una forma de maltrato psicológico, verbal o físico producido entre escolares de forma reiterada y durante un periodo de tiempo determinado, mientras que entiende por *ciberbullying* el maltrato escolar que se comete utilizando la informática e Internet.

[8] Por *sexting* se entiende «el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consienten en ello y, que forma parte de su actividad sexual que se desarrolla de manera libre», que finalmente acaban siendo difundidas, relevadas o cedidas a terceros (Véase, de esta forma, Sentencia número 486/2014 de la Audiencia Provincial de Granada (Sección 1ª), de 18 de septiembre).

[9] Por otro lado, el *child grooming* consiste en el «acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor». Véase, en este sentido, la «Guía S.O.S. contra el Grooming. Padres y educadores», Instituto Nacional de Tecnologías de la Comunicación INTECO), Ministerio de Industria, Energía y Turismo, pág. 5.

perseguir y a que muchos de ellos no están expresamente tipificados en el Código Penal sino remitidos al tipo general, se produzca que el Ordenamiento jurídico no sepa responder ante esta situación, adoleciendo de un gran problema probatorio. Si a eso añadimos que Internet proporciona anonimato a los ciberdelincuentes (por ejemplo, utilizando el navegador *Tor*[10] que hace que la dirección IP no sea revelada) y que el mundo está extremadamente globalizado, ocurre que prácticamente los hechos delictivos no se puedan perseguir y demostrar judicialmente, llegando a situaciones tan inseguras como la atenuación de la pena o la absolución de los acusados. Vivimos en un mundo en el que nos acostamos actualizados, y nos levantamos desactualizados.

Por eso, este Trabajo Fin de Título tiene como objetivo adentrarse en el ámbito de la prueba electrónica, haciéndose especial referencia a su inclusión en el orden jurisdiccional penal. Así, y exponiendo la metodología seguida en este Trabajo, comenzaremos con una explicación teórica sobre esta peculiar figura, en la que nos aproximaremos al concepto y naturaleza jurídica de la prueba electrónica, para después analizar el marco legal aplicable y conocer los requisitos *sine qua non* para que una conversación de *WhatsApp* sea lícita en su obtención. Posteriormente y siguiendo con el orden lógico del proceso, pues hemos decidido que el índice de este Trabajo coincida con él, dado que nos parecía lo más operativo y útil para los Abogados, abordaremos el momento oportuno para proponer y aportar la prueba electrónica, así como las distintas formas de hacerlo, haciendo especial hincapié en la eficacia de cada una de ellas (entre otras, las del «pantallazo»). Asimismo, se estudiará la fase de admisión, práctica y posterior valoración de la prueba, y, para ello, se analizarán los pronunciamientos judiciales más relevantes en la práctica profesional con el objetivo de conocer cuál es la regla general a la hora de valorar la prueba electrónica.

En una última parte, se tratará la cuestión de la autenticidad de la prueba electrónica, y se pondrán encima de la mesa las deficiencias y vulnerabilidades con las que cuenta esta aplicación de mensajería instantánea, pues muchos son los que critican esta figura por su fácil manipulación, afirmación cuya realidad hemos comprobado de manera práctica. Además, se hará una breve referencia a las formas de autenticación de este medio de prueba, en las que será necesario abordar la cuestión del peritaje informático. Por último, se expondrán las conclusiones que se han alcanzado tras el estudio teórico-práctico de la prueba electrónica en el proceso penal, y se propondrá la adaptación/reforma de las leyes procesales con cuestiones de *lege ferenda* para conseguir dar respuesta a estos nuevos escenarios, y conseguir una *Justicia 2.0* que otorgue mayor seguridad jurídica de la que hoy en día existe.

[10] El Navegador *Tor* es una herramienta de *software* diseñada para hacer que las actividades en Internet sean anónimas, teniendo como objetivos principales evadir restricciones electrónicas y ocultar tanto la ubicación así como los sitios que se visitan. Por tanto, toda comunicación que se envía/recibe queda encriptada, provocando que el contenido sea difícil de interceptar. Más información en: https://securityinabox.org/es/tor_principal

II. CONCEPTO, NATURALEZA, MARCO LEGAL, OBTENCIÓN Y LICITUD DE LA PRUEBA ELECTRÓNICA

1. *Aproximación al concepto de prueba electrónica*

El avance tecnológico que ha tenido lugar en estos últimos años ha provocado que nos encontremos ante escenarios jamás nunca vividos; lo que ha ocasionado que las Nuevas Tecnologías se hayan convertido en auténticos instrumentos que intentan probar hechos controvertidos con trascendencia jurídica. Por consiguiente, al cambiar la Sociedad de forma sustancial, han aparecido nuevos medios de comunicación que diariamente cobran especial relevancia (*e-mails*, SMS, *Skype*, *YouTube, Facebook*, *Twitter* e *Instagram*, por citar los más usados), y que no podemos dejar al margen de la realidad jurídica. Además, el uso de los *smartphones* o teléfonos inteligentes mediante su conexión a Internet (por medio de *Wi-Fi* o cobertura móvil 4G, 3G o 2G) ha propiciado el desarrollo de aplicaciones de mensajería instantánea que son masivamente utilizadas para establecer comunicaciones bidireccionales o multidireccionales entre personas[11].

Por consiguiente, las denominadas *apps*, como las señaladas anteriormente: *WhatsApp*, *Allo*, *Line*, *Telegram*, *Hangouts*, *WeChat*, *BlackBerry Messenger*, *Facebook Messenger*, *Viber*, o *Spotbros*, se han convertido en auténticos instrumentos probatorios que se pretenden utilizar en vía judicial. Pues bien, esas nuevas formas de comunicación, en concreto las *apps* –entendidas estas como aplicaciones informáticas diseñadas para ser ejecutadas en teléfonos inteligentes, *tablets* u otros dispositivos móviles con el objetivo de llevar a cabo distintas tareas, como el intercambio de imágenes, documentos, vídeos o información– se perfilan dentro de lo que se ha denominado «prueba electrónica». Y, entre esas nuevas formas de comunicación, destaca por su importancia *WhatsApp*, una aplicación de mensajería instantánea, actualmente gratuita, utilizada en *Smartphones* y otros dispositivos móviles, mediante la cual se pueden enviar y recibir mensajes mediante su conexión a Internet, así como imágenes, vídeos, sonidos o grabaciones de audio.

Así las cosas, lo que aquí nos interesa es que la prueba electrónica se configura como un medio de prueba autónomo que se encuentra amparado por el artículo 299 *in fine* de la Ley 1/2000, de 7 de enero, *de Enjuiciamiento Civil* (a partir de ahora, L.E.C.). Lo importante no es que se analice desde la órbita de fuente de prueba, o sea, de un hecho que se pretende probar en juicio[12], sino como un medio de prueba, pues se configura como «un instrumento conducente a demostrar la certeza de los hechos controvertidos en el proceso»[13]. Es ABEL LLUCH[14] el que hace una

11 Siguiendo la tesis planteada en «Las contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo», Sección Conocimiento, Artículos Doctrinales, *Noticias Jurídicas*, 30 de septiembre de 2015.

12 PÉREZ PALACI, J.E.: *La prueba electrónica: Consideraciones*, 2014, pág. 3 [Recurso electrónico].

13 SÁNCHEZ HERNÁNDEZ, J.: «¿WhatsApp, prueba válida en juicio?», *PorDerecho.com*, nº. 12 – 2016, Revista del Ilustre Colegio de Abogados de Salamanca, págs. 41 – 42.

distinción entre estas dos figuras, pues afirma que será fuente de prueba cuando se pruebe un hecho electrónico –sin entrar en su contenido– (por ejemplo, el envío de un *WhatsApp*), mientras que será medio de prueba cuando haya de probarse electrónicamente un hecho (por ejemplo, que se han llevado a cabo amenazas vía *WhatsApp*). Estas afirmaciones, a pesar de ser verdaderas, pierden importancia cuando al definir prueba electrónica se equipara a documento electrónico, sin tenerse en cuenta que el documento electrónico es únicamente un tipo de prueba electrónica.

Por otro lado, la clave nos la da el artículo 299 *in fine* de la L.E.C. cuando expone que «cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias». O sea, el citado precepto recoge una cláusula abierta por la cual se admiten y recogen tácitamente los medios de prueba no incluidos en el apartado primero del precepto de la L.E.C. –que se presenta como *numerus clausus*–, siempre y cuando se practiquen para la averiguación de hechos relevantes y se tenga absoluta certeza de que otorguen autenticidad a las conversaciones que se intentan aportar en el proceso[15].

En cambio, no nos queda más remedio que, a falta de regulación legal, acudir a los pronunciamientos teórico-prácticos que la doctrina ha ido realizando a lo largo de los años. Y de esta forma, podemos entender por «prueba» aquella «razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de una cosa»[16], o aquel derecho para las partes y aquella obligación para el juez[17]. Sin embargo, no nos podemos quedar ahí, sino que tenemos que aproximarnos al concepto de prueba electrónica (al no existir definición legal), tal y como lo conocemos hoy en día.

Pues bien, uno de los primeros autores en dar un concepto sólido es ILLÁN FERNÁNDEZ, ya que en 2009 la definió desde el punto de vista teórico como «todo soporte magnético, digital o electrónico, creado a través de medios automatizados, capaz de representar una declaración de voluntad, representar hechos, narraciones, datos, cifras, etc., archivado en un soporte electrónico según un formato determinado, el cual sirve para adquirir conocimiento de la certeza de un hecho»[18].

---

[14] GINÉS CASTELLEY. N. (Coord.) y otros: «Prueba electrónica», *La prueba electrónica*, Colección de Formación continua Facultad Derecho ESADE, Serie Estudios Prácticos sobre los medios de prueba, nº 5, Barcelona, 2011, pág. 26.

[15] ILLAN FERNÁNDEZ, J.M.: *La prueba electrónica, eficacia y valoración en el proceso civil*, Navarra, Ed. Aranzadi, 2009, págs. 397 y ss.

[16] SENTIS MELENDO, S.: *La prueba. Los grandes temas del derecho probatorio*, Ed. Ediciones Jurídicas Europa-América, Vol. 65, Buenos Aires, 1979, pág. 35.

[17] CARNELUTTI, F.: *La prueba civil*, 2ª edición, Ed. Ediciones Depalma, Buenos Aires, 2000, págs. 37 y ss.

[18] ILLAN FERNÁNDEZ, J.M.: *La prueba…, op.*, cit, págs. 397 y 398.

Poco después, DE URBANO DE CASTILLO[19] y PÉREZ PALACI[20] dejan la prueba electrónica huérfana de autonomía al enmarcarla dentro del artículo 299.2 de la L.E.C. Esto es, entienden que la prueba electrónica es admitida jurisprudencialmente por tratarse de un medio de «reproducción de la palabra, el sonido y la imagen» así como un instrumento que permite «archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso». Por tanto, consideran que el apartado segundo del citado precepto se configura como un *numerus apertus* completo, cuando en realidad se trata de una remisión al listado recogido en el apartado primero del 299. En otras palabras, la prueba electrónica, entendida como medio de prueba, es completamente autónoma, no dependiendo del listado del artículo 299.1 de la L.E.C.

Pese a todo, es BUENO DE MATA el que en 2014 configura un concepto unánimemente aceptado, pues lo define como «cualquier información obtenida a partir de un dispositivo electrónico o medio digital que sirva para adquirir convencimiento de la certeza de un hecho, siempre que sea correctamente obtenida, constituyendo así pruebas exactas, veraces y objetivas»[21]. Después, puntualiza que se entiende por prueba electrónica «aquel medio electrónico que permite acreditar hechos relevantes para el proceso, ya sean físicos o incluso electrónicos, y que se compone de dos elementos necesarios para su existencia, los cuales delimitan la especialidad de la prueba electrónica en relación al resto de medios probatorios: un elemento técnico o *hardware*, y un elemento lógico o *software*»[22].

Finalmente, DELGADO MARTÍN la define como «toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio»[23]. A pesar de ser una definición poco completa, destaca los siguientes elementos: «se refiere a cualquier clase de información; que ha ser producida, almacenada o transmitida por medios electrónicos; y que pueda tener efectos para acreditar hechos en el proceso abierto para la investigación de todo tipo de infracciones penales, y no solamente para los denominados delitos informáticos. Se acerca así al concepto dado por BUENO DE MATA en 2014.

2. *Sobre la naturaleza de la prueba electrónica: ¿equivalente a la documental?*

A lo largo de los estudios doctrinales, se ha venido caracterizando la prueba electrónica como una prueba puramente documental; y es que se ha asemejado durante muchos años el soporte electrónico con el documento, incluso se ha venido

[19] DE URBANO CASTILLO, E.: *La valoración de la prueba electrónica*, Ed. Tirant lo Blanch, Valencia, 2009, pág. 47.

[20] PÉREZ PALACI, J.E.: *La prueba… op.*, cit, págs. 2-4.

[21] BUENO DE MATA, F.: *Prueba electrónica y proceso 2.0. Especial referencia al proceso civil,* Ed. Tirant lo Blanch, Valencia, 2014, pág. 103.

[22] BUENO DE MATA, F.: *Prueba electrónica… op.*, cit, pág. 103.

[23] DELGADO MARTÍN, J.: «La prueba electrónica en el proceso penal», *Diario La Ley*, nº 8167, Sección Doctrina, Ed. LA LEY, 2013, pág. 1.

aplicando el principio de la equivalencia funcional. Sin embargo, en mi opinión, estas tesis no son del todo válidas, pues la prueba electrónica en sí misma se ha perfilado como una prueba absolutamente autónoma, con especialidades y elementos que hacen de ella una figura *sui generis*. Así las cosas, el punto de partida lo establece el artículo 26 de la Ley Orgánica 10/1995, de 23 de noviembre, *del Código Penal* (a partir de ahora, Código Penal), ya que define documento como «todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica».

En cierto modo, el Legislador ha sido previsor al no vincular exclusivamente documento con papel (esto es, con el soporte tradicional), sino que da pie a nuevos tipos de soporte, como los de carácter informático (USB, CD, discos duros, SMS, y mensajería instantánea, entre otros). Sin embargo, no nos podemos quedar ahí, sino que si por algo destaca la prueba electrónica es por sus elementos. Analicémoslos brevemente[24]:

1. Su soporte goza de carácter material: en este sentido, para su aportación en juicio es necesario que se produzca su lectura; o sea, es preciso que se traduzca el mensaje al lenguaje visual, por lo que lo más importante es la correcta descodificación del mensaje. Por tanto, es necesario que la información que se quiere hacer valer en juicio venga acompañada de la oportuna trascripción; pero, en cualquier caso es recomendable acompañar el dispositivo original de almacenamiento para dar credibilidad y autenticidad a lo aportado.
2. Su contenido es informativo: se pretenden probar datos, hechos o narraciones, así como atribuírselos a una persona (o personas) concreta y determinada. En otras palabras, se trata de aportar información (ya sean conversaciones, audios, grabaciones, imágenes, etc.) que fue enviada por una persona determinada y a la cual se le exigen responsabilidades criminales por su envío. Aquí, es donde nace la discusión de la autoría de la mensajería instantánea, y los problemas que se encuentra la Justicia para demostrar la misma.
3. Esa información necesariamente tiene que tener relevancia jurídica: o sea, tiene que servir para acreditar algún hecho con trascendencia jurídica, y en el orden penal lo suyo es que esa información sirva para acreditar la perpetración de algún hecho delictivo (que se demuestre que existieron amenazas o injurias vía *WhatsApp*, que a través del envío de correos electrónicos se demuestre malversación de caudales públicos, etc.).

[24] Siguiendo la tesis planteada en http://web.icam.es/bucket/ponencia-prueba-electronica.pdf

Siendo fruto de la ausencia de regulación específica, lo cierto es que la naturaleza jurídica de la prueba electrónica plantea problemas teóricos (que alcanzan más tarde a la práctica profesional), hasta tal punto de que son varias las teorías que han nacido al respecto[25]:

- Teoría analógica: aunque minoritaria, esta primera tesis, encabezada por ILLÁN FERNÁNDEZ[26], defiende que existen ciertas similitudes entre la prueba electrónica y la documental. En este sentido, en sus estudios hay una clara remisión a los artículos 328 y ss. de la L.E.C. relativos al deber de exhibición documental entre las partes, consecuencia directa del principio de buena fe procesal[27].
- Teoría autónoma: esta segunda tesis, la más mayoritaria, considera que la prueba electrónica es independiente de la documental, de ahí que obedezca en cierto modo a lo dispuesto en los artículos 299.2, 382, 383 y 384 de la L.E.C.[28]. Y es que si tenemos en cuenta que la prueba electrónica es un elemento que se pretende hacer valer en un proceso, necesita no solo de la licitud en su obtención, sino de la posterior verificación o autenticación de la autoría y de las afirmaciones formuladas. Por eso, estos autores se han remitido a los artículos 299.2, 382, 383 y 384 de la L.E.C., pensando que la prueba electrónica se envuelve dentro de los «instrumentos de filmación, grabación y semejantes», esto es, de los «instrumentos que permiten archivar, conocer o reproducir datos relevantes para el proceso».
- Teoría de la equivalencia funcional: finalmente, esta tesis entiende que «el contenido de un documento electrónico surte los mismos efectos que el contenido de un documento en soporte papel»[29]. En otras palabras, la equivalencia funcional implica «aplicar a los mensajes de datos un principio de no discriminación respecto a las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas; en este sentido los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel o

[25] PEREIRA PUIGVERT, S.: *La exhibición de documentos probatorios y soportes informáticos*, Ed. Aranzadi, Navarra, 2013, págs. 261-262.

[26] ILLÁN FERNÁNDEZ, J.M.: *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil. Nueva Oficina Judicial, Comunicaciones Telemáticas (LEXNET) y el Expediente Judicial Electrónico. Análisis Comparado Legislativo y Jurisprudencial*, Navarra, 2009, págs. 252 y ss.

[27] GINÉS CASTELLEY. N. (Coord.) y otros: «Prueba electrónica… *op.*, cit, pág. 221.

[28] PEREIRA PUIGVERT, S.: *La exhibición… op.*, cit, págs. 257-259.

[29] JURADO SALAZAR, A.: «Valor probatorio del documento electrónico», *Cuestiones Jurídicas, Revista de Ciencias Jurídicas de la Universidad Rafael Urdaneta*, Vol. V, nº 1 (Enero-Junio 2011), Maracaibo, Venezuela, pág. 56.

electrónico donde conste la declaración»[30]. Sin embargo, para que surtan los mismos efectos jurídicos, la Sentencia del Tribunal Superior de Justicia de Andalucía (Málaga), de 28 de enero de 2000 (F.J. 1º) determina que hace falta que el documento se pueda conservar y recuperar, que se pueda traducir al lenguaje común, que se trate de un documento auténtico y que se pueda atribuir su autoría a un sujeto determinado.

Ahora bien, la opinión mayoritaria de la doctrina[31] considera que la L.E.C. en sus artículos 382 - 384, aplica la teoría autónoma, pero la acompaña de ciertas dosis de teoría analógica cuando en su Exposición de Motivos estipula que «podrán confeccionarse y aportarse dictámenes e informes escritos, con sólo apariencia de documentos, pero de índole pericial o testifical y no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales». Pese a ello, nosotros consideramos que la prueba electrónica es una prueba autónoma, independiente y no convencional; y es que dejarla huérfana de autonomía sería provocar mayor inseguridad jurídica de la que hoy en día existe. Dicho de otra forma, la prueba electrónica en sí misma no puede ser enmarcada dentro del artículo 299.2 de la L.E.C., pues no se trata de un medio de «reproducción de la palabra, el sonido y la imagen» ni de un instrumento que permite «archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso», sino que se trata de un medio al cual se le aplica el apartado tercero del artículo 299.

En este sentido, el apartado segundo del citado precepto hace una remisión al listado recogido en su apartado primero, y lo cierto es que la prueba electrónica no depende de ese listado (o sea, no tiene por qué constituirse como prueba de interrogatorio de las partes, prueba testifical o prueba pericial). Por el contrario, se trata de un medio de prueba que se introduce dentro de la cláusula abierta que recoge el apartado tercero, ya que, al no contar con una regulación específica en esta materia, la cobertura jurídica tiene que ser otorgada por un precepto que haga las veces de cajón de sastre. Así, «cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias».

Hay mucho camino que recorrer, y muchos obstáculos que sortear; pero, lo más idóneo sería establecer una nueva regulación del artículo 299 de la L.E.C. Para ello, BUENO DE MATA propone que su apartado segundo quede de la siguiente manera:

[30] SOTO CALDERA, M.M.: «Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano», *Estudios de derecho civil*, Vol. III, Libro homenaje a José Luis Aguilar Gorrondona, Tribunal Supremo de Justicia, Colección Libros homenaje nº. 5, 2001, pág. 663.

[31] PEREIRA PUIGVERT, S.: *La exhibición… op.*, cit, pág. 262.

«También se admitirá cualquier fuente de prueba que pudiera ser originada por el desarrollo tecnológico, científico o informático, la cual será incorporada a través de los medios probatorios regulados en el apartado anterior, siempre que de ellas pudiera obtenerse certeza sobre hechos relevantes. El tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias para su correcta incorporación al proceso»[32].

De esta forma, esta redacción se aleja del *numerus clausus* del artículo 299.1 de la L.E.C. para avanzar hacia una apertura en su apartado segundo, con el objetivo de adelantarse a los nuevos acontecimientos sociales, económicos, tecnológicos, etc. que pudieran darse durante los próximos años. En este sentido, estamos de acuerdo con la propuesta de regulación que realiza BUENO DE MATA, pues hay que adaptar nuestra Justicia a la realidad social que vivimos.

3. *Marco legal aplicable: de la ausencia de normativa específica*

Tal y como se expuso con anterioridad, no existe una regulación específica, completa, real y eficaz para este tipo de medio probatorio, por lo que no nos queda más remedio que acudir a la regulación clásica y aplicar esta por pura analogía. Sin embargo, aplicar por analogía una regulación con una redacción tan general hace, usaremos un símil, que luchemos contra una devastadora enfermedad empleando un mero placebo. Así, este vacío legislativo genera una elevada inseguridad jurídica, de ahí que resulte necesario realizar una breve referencia a la normativa comunitaria y a la internacional para ponerla en consonancia con nuestra legislación estatal.

3.1. Normativa estatal

A este hándicap, hay que añadirle el hecho de que en el Real Decreto de 14 de septiembre de 1882, *aprobatorio de la Ley de Enjuiciamiento Criminal* (a partir de ahora, L.E.Crim.) no se haga ni la más mínima referencia a la prueba electrónica, de ahí que en este Trabajo se haya aludido anteriormente a preceptos que regulan los procesos civiles. No queda, pues, más remedio que acudir a la L.E.C., aplicando el principio de supletoriedad que recoge nuestro Ordenamiento.

Así, el artículo 4 de la L.E.C. nos da la cobertura jurídica necesaria para poder hablar hoy en día de la prueba electrónica y de sus efectos, al estipular que «en defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley». Dicho esto, el punto de partida, como no podía ser de otra manera, lo constituye nuestra Constitución, pues en su artículo 24 apartado segundo consagra que «todos tienen derecho […] a utilizar los medios de prueba pertinentes para su defensa […]». Por consiguiente, la prueba en sí, y por ende la electrónica, se ha consagrado por el Legislador como un derecho fundamental al que todas las personas tienen acceso, garantizando así a las partes la posibilidad de impulsar una actividad probatoria acorde con sus

[32] BUENO DE MATA, F.: *Prueba electrónica… op.*, cit, págs. 117 y ss.

intereses (véanse, SSTC 173/2000, de 26 de junio –F.J. 3º–, y 1/2004, de 14 de enero –F.J 2º–). Y esto tiene relevancia a la hora de analizar la licitud en la obtención de los mensajes de *WhatsApp* a la hora de aportarlos en el proceso.

Como se ha analizado anteriormente, la prueba electrónica tiene su razón de ser en el contenido del artículo 299.3 de la L.E.C., pues se trata de un medio no expresamente previsto en los apartados anteriores del artículo citado pero que potestativamente el Tribunal, a instancia de parte, puede admitirlo como prueba siempre y cuando se pudiera tener certeza sobre hechos relevantes que se discuten en el proceso. Se trata, como ya se ha apuntado, de un *numerus apertus* o cláusula abierta, que permite la incorporación al proceso de nuevas fuentes de prueba, así como de nuevos medios de prueba. Sin embargo, la redacción del precepto no ha quedado exenta de polémica pues autores, como ABEL LLUCH, entienden que «cuando el artículo 299.3 LEC alude literalmente a "cualquier otro *medio* no expresamente previsto en los apartados anteriores", se está refiriendo, en puridad procesal, a cualquier otra *fuente* de prueba, puesto que los medios son limitados y las fuentes ilimitadas»[33].

Esto es, el Legislador no distingue medios de prueba y fuentes de prueba, y los mete en el mismo compartimiento. Esta tesis la sigue en los mismos términos la Audiencia Provincial de Barcelona en Sentencia de 2 de mayo de 2007, ya que afirma que «con la L.E.C., se regulan un conjunto de "medios de prueba" (aunque en realidad son "fuentes" de prueba) cuya característica común es la capacidad para retener palabras y/o imágenes que se desarrollaron en un momento determinado, con posibilidad de reproducirlas después, facilitándose la oralidad, la inmediación y la concentración». A pesar de todo, la cláusula del apartado tercero del 299 es un claro reflejo del derecho a la utilización de los medios de prueba pertinentes, que recoge nuestra Constitución en el artículo 24.2.

Así las cosas, se trata de una «apertura legal a la realidad de cuanto puede ser conducente para fundar un juicio de certeza sobre las alegaciones fácticas, apertura incompatible con la idea de un número cerrado y determinado de medios de prueba»[34]; versión que se corrobora cuando en la Exposición de Motivos de la L.E.C., tal y como se apuntaba anteriormente, se afirma que «podrán confeccionarse y aportarse dictámenes e informes escritos, con sólo apariencia de documentos, pero de índole pericial o testifical y no es de excluir, sino que la ley lo prevé, la utilización de nuevos instrumentos probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales».

[33] GINÉS CASTELLEY. N. (Coord.) y otros, «Prueba electrónica… *op.*, cit, págs. 96 -97.

[34] GINÉS CASTELLEY. N. (Coord.) y otros, «Prueba electrónica.… *op.*, cit, págs. 97 -98.

Después, el artículo 299 se pone en relación con los artículos 382 a 384. de la L.E.C.; pero, a pesar de que en la práctica a la mensajería instantánea se le aplica esta regulación para darle valor probatorio, lo cierto es que no se envuelve dentro de los «instrumentos de filmación, grabación y semejantes» que recoge el apartado segundo del 299, esto es, de los «instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso». Por ello, en nuestra opinión, se necesita de una regulación concreta y específica para otorgar mayor seguridad jurídica al proceso penal; y es que esos preceptos recogen los «nuevos medios» de prueba, pero en ningún momento la L.E.C. menciona a la prueba electrónica ni tan siquiera al documento electrónico.

Esa aplicación práctica poco segura también ocurre con respecto al artículo 333 de la L.E.C., ya que a la hora de realizarse copias de documentos que no incorporan predominantemente textos escritos o que se han realizado por medios electrónicos se dará fe de la autenticidad de las copias por la Oficina Judicial correspondiente[35]. Sin embargo, la L.E.C. no menciona de nuevo la prueba electrónica ni el documento electrónico.

Por otra parte, el Legislador podría haber acabado con ese vacío legislativo, aunque de una manera poco eficaz, o sea, sin reformar la L.E.C. podía haber elaborado nuevas Leyes que suplieran esta falta de contenido. Pero, no lo ha hecho. A lo largo de este siglo, han sido numerosas las Leyes que han rellanado ciertos vacíos legales, provocados por la evolución de la Sociedad y de la Tecnología, pero no en lo que se refiere a la prueba electrónica. Hagamos así referencia a las que tienen aplicación indirecta sobre la materia que nos ocupa.

Una de las primeras Leyes en aparecer fue la Ley 34/2002, de 11 de julio, de *Sociedad de Servicios de la Información y de Comercio Electrónico*. En su artículo 24, se admite «el soporte electrónico en que conste un contrato celebrado por vía electrónica» como prueba documental. Además, la Ley 59/2003, de 19 de diciembre, *de firma electrónica* se ha encargado de delimitar una vez más lo que se entiende por firma electrónica, para después hacerlo con respecto al documento electrónico, al cual ha categorizado de prueba documental. Entre sus novedades, destaca el hecho de que haya incluido métodos para salvaguardar la autenticidad de la firma electrónica en caso de ser impugnada en el proceso.

Otras leyes, fruto de las exigencias de transposición de Directivas provenientes de la Unión Europea, tales como la Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*, la Ley 9/2014, de 9

[35] **Artículo 333 Extracción de copias de documentos que no sean textos escritos: «**Cuando se trate de dibujos, fotografías, croquis, planos, mapas y otros documentos que no incorporen predominantemente textos escritos, si sólo existiese el original, la parte podrá solicitar que en la exhibición se obtenga copia, a presencia del secretario judicial, que dará fe de ser fiel y exacta reproducción del original. Si estos documentos se aportan de forma electrónica, las copias realizadas por medios electrónicos por la oficina judicial tendrán la consideración de copias auténticas».

de mayo, *General de Telecomunicaciones* o la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, se aplican también de forma indirecta en esta materia.

Como se puede observar, no existe una regulación específica en esta materia, ni en la L.E.Crim., ni en la L.E.C. en su aplicación supletoria, ni tampoco en ninguna norma con rango de Ley. Por ello, resulta necesario abandonar la aplicación análoga, y regular expresamente el acceso a la información contenida en dispositivos electrónicos y su incorporación al proceso penal, eliminando incertidumbres con pleno respeto a las garantías del proceso[36].

También, cabe destacar que con motivo de la Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2011, España se ha visto obligada a cumplir su contenido, por lo que ha resultado necesario luchar contra los delitos informáticos, así como proveer los medios para la obtención de las pruebas electrónicas en cualquier delito. Así pues, en su artículo 14 se estipula que «cada Parte adoptará las medidas legislativas», entre otras la de los delitos cometidos por medio de un sistema informático y la de la obtención de pruebas electrónicas de un delito. Fruto de todo ello, se elaboró Propuesta de Texto Articulado de Ley de Enjuiciamiento Criminal, por la Comisión Institucional creada por Acuerdo de Consejo de Ministros de 2 de marzo de 2012[37], en la que se estudió la posibilidad de incluir un Capítulo en el que regulara el «Registro de dispositivos de almacenamiento masivo de información» (arts. 347 y ss.) y otro Capítulo relativo a los «Registros remotos sobre equipos informáticos» (arts. 350 y ss.).

Finalmente, la Propuesta salió adelante mediante Ley Orgánica 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. Así, ha establecido nuevos medios para avanzar hacia la agilidad procesal para la obtención de pruebas. Por tanto, la L.E.Crim. fue reformada, añadiendo los Capítulos VIII y IX del Título VIII («Registro de dispositivos de almacenamiento masivo de información» –arts. 588 *sexies* a y ss. – y «Registros remotos sobre equipos informáticos» –arts. 588 *septies* a y ss. –).

Quizá lo más importante es la exigencia del deber de colaboración que se incluye en el artículo 588 *septies* b, ya que «los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida

[36] DELGADO MARTÍN, J.: *La prueba electrónica… op.*, cit, págs. 1 y 2.

[37] http://www.mjusticia.gob.es/cs/Satellite/Portal/1292387342364?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DPropuesta_texto_articulado_L.E.Crim..PDF

y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización». Posteriormente, se analizará el alcance de esta legislación.

El Legislador, también, ha querido que se haga un «uso generalizado de los medios electrónicos como forma normal de tramitación de los procesos judiciales y de relacionarse la Administración de Justicia con los profesionales y con los ciudadanos» (Exposición de Motivos). Por ello, reforma en profundidad el modo de realizar las diferentes actuaciones procesales, dando así mayor relevancia al uso de los medios telemáticos o electrónicos, y lo hace a través de la promulgación de la Ley 42/2015, de 5 de octubre, *de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil*.

Por último, cabe destacar la ambición extrema de nuestro Legislador para modernizar y agilizar la Justicia, tanto es así que mediante Real Decreto 1065/2015, de 27 de noviembre, *sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET*, desarrolla la implantación del sistema «LExNET», que tanto quebraderos de cabeza lleva a los operadores jurídicos, para dar aplicación a la Ley 18/2011, de 5 de julio, *reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.*

3.2. Normativa comunitaria

A priori, países como Austria, Dinamarca o Suecia incluyen en su legislación una mayor apertura en lo que se refiere a los nuevos medios de prueba pues basan su modelo en el principio de la libre valoración del juez. Sin embargo, lo cierto es que la mayoría de los Estados miembros de la Unión Europea dan prioridad a los medios de prueba tradicionales. Como consecuencia de esta diversidad legislativa, en el seno de la U.E. se ha elaborado normativa especialmente importante para nuestro país, pero ninguna en relación a lo que puramente es prueba electrónica (y que ha dado como resultado las anteriores Leyes).

Sin embargo, conviene advertir que el *Convenio Europeo de Derechos Humanos* consagra en su artículo 8.1 el derecho al respecto de la vida privada y familiar, lo que nos puede servir a la hora de analizar si la obtención de un mensaje de *WhatsApp* se ha llevado a cabo con la licitud exigida.

3.3. Normativa internacional

Tampoco, los organismos internacionales han sido capaces de unificar los criterios aplicables a la prueba electrónica y dar una respuesta válida a este gran problema. A pesar de ello, la Asamblea General de la Organización de las Naciones Unidas adoptó Resoluciones 55/63 y 56/121 (Lucha contra la Utilización de la Tecnología de la Información con fines delictivos) sobre el

combate contra el mal uso de las Nuevas Tecnologías de la información, destacando «la necesidad de garantizar que cada país miembro adapte sus leyes para eliminar el ciberespacio de la delincuencia, intercambiando la información entre los estados y cooperar y coordinar a fin de una buena investigación penal concreta contra el mal uso de las TIC»[38]. Pese a ello, poco se ha luchado contra las amenazas de la ciberdelincuencia.

4. *Obtención de la mensajería instantánea como medio de prueba: el juicio de licitud*

Anteriormente, se ha expuesto que la utilización de los medios de prueba pertinentes para la defensa de las partes intervinientes en el proceso se ha consagrado como derecho fundamental en el artículo 24.2 de nuestra Carta Magna. Por tanto, nuestro Ordenamiento ha previsto que, a la hora de obtenerse una prueba, se haga un juicio previo de licitud, con el objetivo de que se asegure que la obtención de esa prueba se hizo con respeto a la Ley y sin dañar los derechos fundamentales. Así las cosas, para que una prueba electrónica sea lícita es necesario que:

a. **Que se cumplan los requisitos de los artículos 281 y 283 de la L.E.C.**: puede parecer una obviedad, pero la prueba electrónica tiene que ser necesariamente pertinente (o sea, que guarde estrecha relación con el objeto del proceso), útil (esto es, que vaya encaminada a esclarecer los hechos) y debe haber sido obtenida de forma lícita[39]. En otras palabras, «la prueba tendrá como objeto los hechos que guarden relación con la tutela judicial que se pretenda obtener en el proceso» (artículo 281.1 de la L.E.C.), «no deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente» (artículo 283.1 de la L.E.C.), «tampoco deben admitirse, por inútiles, aquellas pruebas que, según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos» (artículo 283.2 de la L.E.C.), y «nunca se admitirá como prueba cualquier actividad prohibida por la ley» (artículo 283.3 de la L.E.C.).

   Sobre lo que más discusión doctrinal ha habido es respecto de la pertinencia de la prueba, por eso incidiremos en el tema. Pues bien, es conveniente conocer el alcance práctico del derecho a la utilización de los medios de prueba pertinentes para la defensa de las partes procesales, y para ello tendremos que acudir a la jurisprudencia.

   Así pues, el Tribunal Constitucional en Sentencias número 147/2002, de 15 de junio – F.J. 4º– y 70/2002, de 3 de abril –F.J. 5º–; ha entendido que se hará legítimo uso de los medios de prueba cuando se pretenda practicar pruebas relacionadas con el *thema decidendi*, o sea, el tema que debe de decidirse. En caso de que ese uso fuera más allá del tema que se está decidiendo, se produciría una dilación indebida en el proceso y, por ende, una vulneración del artículo 24.2 de la Constitución Española (véase Auto del Tribunal Constitucional

[38] PÉREZ PALACI, J.E., *La prueba… op.,* cit, pág. 2.

[39] SÁNCHEZ HERNÁNDEZ, J., «¿WhatsApp, prueba… *op.*, cit, págs. 42 – 43.

número 569/1983, de 23 de noviembre – F.J. 6º–). En el caso que nos ocupa, una prueba será pertinente cuando, por ejemplo, se aporte una conversación de *WhatsApp* a un proceso donde se discute la realización de un delito de *ciberbullying*.

b. **Que la prueba se haya solicitado diligentemente:** en consonancia con lo anteriormente expuesto, la prueba electrónica tiene que haberse solicitado en la forma y momento legalmente establecidos (véase Sentencia del Tribunal Constitucional número 173/2000, de 26 de junio –F.J. 3º–); teniendo en cuenta además que el medio de prueba en sí debe estar autorizado por el Ordenamiento. Pues bien, la prueba electrónica sería un medio de prueba válido para ser aportado en un proceso, dado que tiene cabida en el artículo 299.3 de la L.E.C. Y junto a ello, es necesario que la parte que la solicita tenga la legitimación suficiente como para hacerlo (véase Sentencia del Tribunal Constitucional número 236/2002, de 9 de diciembre –F.J. 4º–).

c. **Que la prueba tenga relevancia jurídica:** otro de los requisitos necesarios es que acredite algún hecho con trascendencia jurídica, esto es, que tenga una influencia decisiva en la resolución del pleito (véase Sentencia del Tribunal Constitucional número 70/2002, de 3 de abril –F.J. 5º–).

d. **Que se cumpla con el contenido del artículo 11 de la Ley Orgánica 6/1985, de 1 de julio, *del Poder Judicial***: reza este precepto que «en todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». O sea, es necesario «que en su obtención no se hayan vulnerado ni el derecho a la intimidad ni el secreto de las comunicaciones»[40]. Así pues, no se debe vulnerar ningún derecho fundamental; en caso contrario, la obtención será ilícita, y, por ende, la prueba también.

e. **Que se respete el derecho a la intimidad personal y la autodeterminación informativa**: consagra la Constitución Española en su artículo 18.1 que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Del mismo modo, su apartado cuarto reza que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Fruto de ese contenido, se desarrolló la Ley Orgánica 1/1982, de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*, de ahí que «la propuesta en un proceso de contenidos de mensajes de un sistema de mensajería instantánea como medio de prueba, no podrá vulnerar el artículo 7»[41] de la Ley Orgánica citada anteriormente.

[40] BACARIA MARTRUS, J.: «El caso WhatsApp. Las aplicaciones de mensajería instantánea como medio de prueba en el procedimiento judicial», *Economist & Jurist*, Vol. 22, nº 185, noviembre 2014, pág. 82.

[41] BACARIA MARTRUS, J.: «El caso WhatsApp… *op*., cit, pág. 83.

Una vez más tenemos que acudir a los pronunciamientos doctrinales para saber el alcance de este derecho. Así pues, la Sentencia del Tribunal Constitucional número 11/1984, de 29 de noviembre, extiende su alcance hasta tal punto de que «quien graba una conversación de otros, atenta, independientemente de toda otra consideración, al derecho reconocido en el artículo 18.3 CE; por el contrario, quien graba una conversación con otro, no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado».

f. **Que se respete el derecho al secreto de las comunicaciones**: del mismo modo, la Constitución Española establece en el apartado tercero de su artículo 18 que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial». Como nos encontramos analizando la obtención de la prueba electrónica en el proceso penal, tenemos que tener en cuenta que los delitos se pueden perseguir de oficio (véanse artículos 259 y ss. de la L.E.Crim.), de ahí que durante la fase de investigación o instrucción también se tenga que salvaguardar la licitud de la obtención de las pruebas.

   Por consiguiente, «los mensajes de móvil como medio de prueba deberán respetar el derecho fundamental al secreto de las comunicaciones, derecho que tiene una entidad propia, cuya regulación también la encontramos en el artículo 197 del Código Penal, diferenciada del derecho a la intimidad, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido»[42]. Una vez más, el Tribunal Constitucional en su Sentencia número 70/2002, de 3 de abril, sostiene que alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la interferencia o intervención de la comunicación de cualquier persona, convertirá la prueba en ilícita, y podrá constituir un delito, salvo que se realice mediante resolución judicial y con las garantías legalmente previstas.

   Así, por ejemplo, no se podría considerar lícita la aportación por parte de un agente de la autoridad, en caso de no tener autorización judicial para ello, de grabaciones realizadas desde *WhatsApp*, tras la intercepción ilegal de un teléfono dónde se reconoce la propiedad de numerosas armas conseguidas en el mercado negro, pues la prueba fue obtenida de forma ilícita al ponerse el peligro el derecho al secreto de las comunicaciones. La Fiscalía General del Estado ha sido consciente del estrecho margen de actuación con el que cuentan las Fuerzas y Cuerpos de Seguridad del Estado, de ahí mediante Circular 1/2013 haya establecido ciertas pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Entre otras cuestiones, afirma que «las intervenciones telefónicas tienen una doble naturaleza en el proceso penal: 1) pueden servir de fuente de investigación de delitos, orientando la encuesta policial y 2) pueden utilizarse como medio de prueba (STS nº 511/1999, de 24

[42] BACARIA MARTRUS, J.: «El caso WhatsApp… *op*., cit, págs. 83 y 84.

de marzo). En ambos casos se requiere como exigencia indefectible la observancia de una serie de requisitos que garantizan que la invasión o injerencia en el ámbito de la intimidad personal que protege el art. 18 CE se lleva a cabo de manera constitucionalmente correcta» (Apartado 3). Por tanto, siendo consciente de la relevancia de la prueba electrónica en el orden jurisdiccional penal, pide actuar con diligencia en la intervención de las comunicaciones, pues una mala aplicación de los protocolos puede hacer de una prueba decisiva una prueba ilícita.

Finalmente, cabe destacar que a través del Sistema Integrado de Interceptación de Telecomunicaciones (más conocido como S.I.T.E.L.) ya se contempla la posibilidad no solo de intervenir las llamadas, mensajes de texto, etc. del dispositivo móvil de un presunto delincuente, sino que también se tendrá acceso, mediante autorización judicial, a todo el contenido de las aplicaciones instaladas en el terminal (entre otras, *WhatsApp*). Se aplica así lo contenido en los artículos 588 *ter* a y ss. de la L.E.Crim., dónde «se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga».

g. **Que se respete el derecho a la inviolabilidad domiciliaría:** fruto del deber de persecución de oficio de los delitos públicos, también se tiene que cumplir fielmente lo dispuesto en el apartado segundo del artículo 18 cuando reza que «el domicilio es inviolable» y que «ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito». Y, en este sentido, por domicilio se entiende «un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima»[43]. Por ello, a través de este derecho no solo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de la esfera privada de ella»[44]. Así las cosas, por ejemplo, no se podrían aportar imágenes realizadas desde *WhatsApp* por parte de un agente de la autoridad que se introduce en un domicilio sin la autorización judicial oportuna aprovechando que no hay nadie, en el caso de que dentro de un domicilio particular se tengan plantas de marihuana para su distribución y venta, pues la prueba fue obtenida de forma ilícita al ponerse el peligro el derecho a la inviolabilidad domiciliaria.

   El Tribunal Supremo se ha encargado recientemente, mediante Sentencia de la Sala II 329/2016, de 20 de abril, de configurar el alcance de este derecho. En un supuesto de tráfico de drogas, el Tribunal Supremo anula la condena de cárcel interpuesta a dos personas, pues entiende que hubo vulneración del

[43] Véase, en este sentido, Sentencia del Pleno del Tribunal Constitucional número 10/2002 –F.J. 6º–.

[44] Siguiendo la tesis planteada en la Sentencia del Tribunal Constitucional número 22/1984 –F.J. 5º–.

artículo 18.2 de la Constitución Española por el hecho de que los agentes de la autoridad que investigaban los hechos utilizaron prismáticos con el objetivo de conocer la actividad ilícita de los acusados. En este sentido, entiende que «la protección constitucional de la inviolabilidad del domicilio, cuando los agentes utilizan instrumentos ópticos que convierten la lejanía en proximidad, no puede ser neutralizada con el argumento de que el propio morador no ha colocado obstáculos que impidan la visión exterior » (F.J. 2º).

Además, establece que «el art. 588 quinquies a), introducido por la reforma de la LO 13/2015, 5 de octubre, en su apartado 1º dispone que "la Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos". Sin embargo, el art. 588 quater a) somete a autorización judicial la utilización de dispositivos electrónicos orientados a la grabación de imágenes o de las comunicaciones orales directas entre ciudadanos que estén siendo investigados, ya se encuentren aquéllos en un recinto domiciliario, ya en un lugar público».

h. **Que se preserve la cadena de custodia**: de nuevo, al tratarse de delitos públicos, hay que tener en cuenta que debe preservarse la cadena de custodia en la obtención y la conservación de la prueba, elemento fundamental para la validez y admisibilidad de los mensajes de móvil. Así, se debe garantizar en todo momento la autenticidad e integridad del medio probatorio, ya que si, por ejemplo, se interviene un teléfono móvil de un narcotraficante se tiene que conservar la información que reside en él, pues a través de las conversaciones que tiene en *WhatsApp* se puede demostrar que realiza envíos de droga procedentes de Colombia con destino al Aeropuerto Madrid-Barajas Adolfo Suárez. Por ello, la Sentencia del Tribunal Constitucional de 29 de septiembre de 2003 resulta de aplicación, pues establece ciertos requisitos que deben cumplirse en el supuesto de que algo se incaute, con el objetivo de que no se produzca su manipulación. Así pues, es necesario que se describan los materiales incautados en la Diligencia del Letrado de la Administración de Justicia (póngase en relación con el artículo 334 L.E.Crim.), que dicha custodia se realice en un lugar adecuado (para evitar su destrucción, deterioro o manipulación), y que exista un control judicial tanto en la recogida como en la custodia de esas pruebas. En el caso de que estos requisitos no se cumpliesen, no se respetarían las garantías esenciales del proceso judicial y el derecho de defensa se vería gravemente afectado.

III. DE LA APORTACIÓN DE LA PRUEBA ELECTRÓNICA EN EL PROCESO PENAL

1. *Relevancia de la prueba electrónica en el orden jurisdiccional penal*

Las T.I.C.S. han provocado que la prueba electrónica haya adquirido mayor relevancia en el orden jurisdiccional penal, pues al tiempo que surgen nuevos medios de comunicación, se desarrollan nuevas formas de delinquir, a las cuales tampoco se les puede dar una respuesta jurídica eficaz, dado que nuestro Código Penal todavía no ha sido actualizado eficientemente a los nuevos tiempos. Así, el crecimiento de los *ciberdelitos* o delitos informáticos ha ocasionado que sea muy importante la aportación de la prueba electrónica en el proceso penal, en detrimento de la prueba tradicional. Uno de los delitos informáticos más extendidos entre los menores de edad es el *ciberbullying*, pues a través de la aplicación *WhatsApp* se han creado conversaciones multidireccionales –grupos– con el objetivo de insultar, amenazar y amedrentar a la víctima que sufre este tipo de acoso. También, la prueba electrónica ha adquirido cierta importancia en delitos como la violencia de género, pues es desgraciadamente habitual emplear *WhatsApp* para amenazar y coaccionar a la víctima de violencia de género y someterla a un mayor control y dominación.

Así las cosas, lo cierto es que los medios de prueba que se encuentran amparados por el apartado tercero del artículo 299 de la L.E.C. adquieren con el paso del tiempo mayor importancia, en detrimento de los medios de prueba tradicionales. Y es que la prueba electrónica permite en muchos casos acreditar frente a la Justicia actos, comunicaciones y hechos que tienen cierta relevancia jurídica. Por consiguiente, el soporte en papel pierde relevancia en un entorno cada vez más virtual, dónde existen instrumentos como el SMS, el USB, las grabaciones de voz y vídeo y los *e-mails*. Pero, estos nuevos medios de prueba no quedan exentos de polémica, pues muchas veces es difícil demostrar la autoría de esos actos, comunicaciones y hechos, así como la autenticidad de los mismos. Nos encontramos, pues, ante medios intangibles y volátiles, que pueden ser fácilmente copiados, manipulados y reproducidos.

Pero, ¿hasta qué punto es relevante la prueba electrónica en el proceso penal? Pues bien, en los últimos años han sido numerosos los casos que han dejado en evidencia la importancia de la prueba electrónica. Uno de los asuntos más mediáticos fue el denominado «Caso Olvido Hormigos», ya que Olvido Hormigos, entonces Concejala de Los Yébenes (Toledo) formuló denuncia por la presunta comisión de una falta de injurias y vejaciones y un presunto delito contra la integridad moral del artículo 197 del Código Penal, por la divulgación de dos vídeos de contenido sexual grabados en su domicilio, uno de ellos enviado por correo electrónico y otro por el teléfono móvil a través de la plataforma de mensajería *WhatsApp*. Finalmente, a través de Auto del Juzgado de Primera Instancia e Instrucción nº 1, de fecha 15 de marzo de 2013, que pone fin a las Diligencias Previas 1109/2012 se decreta archivo provisional de las actuaciones al no constatarse delito contra la intimidad ya que «la víctima confeccionó voluntariamente el referido vídeo en la privacidad de su domicilio, usando al efecto su teléfono móvil, y posteriormente, lo envió al imputado

(actualmente, investigado), concurriendo igual voluntariedad y ánimo, en diversas ocasiones. Este elemento subjetivo o volitivo, esto es, la plena voluntariedad y consentimiento de la denunciante en el envío del citado vídeo a través de su teléfono móvil al imputado, quiebra desde el inicio la posible subsunción de los hechos denunciados en un delito contra la intimidad» (F.J. 2º). Sin embargo, la conducta todavía no ha sido castigada, a pesar de que los videos accedieron a numerosas redes sociales de contenido público. Fruto de esta falta de concreción penal, la Ley Orgánica 1/2015, de 30 de marzo, *por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal* introdujo el apartado 7 del artículo 197 para dar solución a este tipo de vacíos legales[45].

Además, la Sentencia número 587/2014 de la Sala de lo Penal del Tribunal Supremo, que confirma la Sentencia de Audiencia Provincial de Córdoba, de fecha 5 de noviembre de 2013, y la Sentencia número 43/2013 de la Sala Civil y Penal del Tribunal Superior de Justicia de Andalucía, se valió de diversas pruebas electrónicas para condenar a don José Bretón Gómez, como autor criminalmente responsable de dos delitos de asesinato, con la concurrencia en ambos de la circunstancia agravante de parentesco, a las penas, por cada asesinato, de veinte años de prisión. En este sentido, el condenado fue delatado gracias al análisis de la información almacenada en su *iPhone*, pues, entre otras cosas, se demostró pericialmente que se había procedido al borrado de más de 50 registros de llamadas. Y, de las informaciones *Wi-Fi* y de las antenas *BTS* registradas en el terminal del padre de los menores, se comprobó que estuvo numerosos días en la finca *Las Quemadillas*, lugar del crimen, incluso que se pudo saber que su terminal fue apagado el día en el que cometieron los hechos delictivos. Además, se aportaron en juicio las llamadas y conversaciones que Bretón llevó a cabo para simular la desaparición de sus hijos.

Por otra parte, la prueba electrónica adquirió relevancia en el llamado «Caso Asunta». Y es que la Sentencia 365/2015, de 11 de noviembre, de la Audiencia Provincial (Sección 6ª) de A Coruña, confirmada el pasado marzo por el Tribunal Superior de Justicia de Galicia y en octubre por el Tribunal Supremo, condena a 18 años de prisión a don Alfonso Basterra Amporro y a doña Rosario Porto Ortega como autores responsables de un delito de asesinato. Quedó probado que ambos suministraron durante varios meses a su hija, doña Asunta Yong Fang Basterra Porto, *lorazepam*, un medicamento que produce somnolencia y sedación. Finalmente, y en estado de sedación, los progenitores asfixiaron a su hija, la cual no pudo defenderse pues estaba bajo los efectos del medicamento (Antecedente de Hecho 11º). Para la resolución del caso, cobraron especial relevancia las conversaciones que ambos progenitores habían mantenido con sus dispositivos móviles (muchas de ellas habían sido eliminadas), así

[45] **Artículo 197 apartado 7º**: «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona».

como la práctica de los informes periciales en los que se demostró la posición exacta de los dispositivos móviles a través de los repetidores de telefonía.

Finalmente, hay que destacar que la prueba electrónica ha adquirido especial relevancia en el «Caso Nóos», en el «Caso Diana Quer» y en el «Caso del Asesino de Pioz», procesos judiciales aún abiertos. Así, en el primero se han aportado numerosos correos electrónicos por parte de don Diego Torres, ex-socio de don Iñaki Urdangarin, con el objetivo de inculpar tanto a este como a la Casa Real por los delitos de malversación, fraude fiscal, prevaricación, falsedad documental y blanqueo de capitales. También, en el segundo, se ha demostrado por parte de la Guardia Civil que la joven desaparecida pudo viajar a Taragoña (A Coruña), localidad próxima a A Pobra do Caramiñal, lugar dónde se cree que desapareció. La investigación tecnológica demuestra que mediante el análisis de la señal que emiten los repetidores de telefonía se puede situar con exactitud la ubicación del teléfono móvil de la joven. Asimismo, se intuye que dada la proximidad de la señal de los repetidores de A Pobra do Caramiñal y posteriormente de Taragoña el terminal tuvo que ser transportado en un vehículo, pues esa distancia (aproximadamente, unos 20 kilómetros) no se podía realizar en otro medio de transporte. También, la investigación se ha centrado en rastrear los móviles que hiciesen el mismo recorrido que el teléfono de la joven.

Por último, en el «Caso del Asesino de Pioz» se analizaron tanto la posición del teléfono móvil del sospechoso como los movimientos registrados en la tarjeta de abono del transporte público que este tenía en su propiedad. Así, la investigación se centró en analizar las notas de voz, las imágenes y las conversaciones que el presunto asesino había mantenido con uno de sus amigos a través de la aplicación *WhatsApp*, lo que demostró que a través de la geolocalización de su terminal el presunto asesino se situaba en la vivienda y en el periodo de tiempo en el que se produjeron los asesinatos. Finalmente, el presunto autor de los hechos, Patrick Gouveia, se entregaría a las autoridades para evitar su extradición a España.

2. *Momento de proposición y aportación de la prueba electrónica en el proceso penal*

Si por algo destaca el orden jurisdiccional penal es porque la proposición y la aportación de la prueba, para su posterior admisión, práctica y valoración, cobra especial importancia a la hora de acreditar hechos que se introducen dentro de la redacción de los diferentes tipos penales. Dicho de otra manera, el momento de proposición y aportación de la prueba penal forma parte de la estrategia del Ministerio Fiscal, de la acusación o, en su caso, de la defensa. Surgen, por tanto, dudas acerca de cuándo debe aportarse la prueba en el proceso penal, entendiendo este trámite como «aquel acto procesal por el cual se indica al juzgador o a los miembros del tribunal el medio o medios de prueba que se pretenden utilizar para obtener la convicción del juez»[46].

[46] BUENO DE MATA, F.: *Prueba electrónica.…*, op. cit, pág. 199.

Pues bien, el punto de partida lo constituye el artículo 656 de la L.E.Crim., ya que se encarga de establecer que «el Ministerio Fiscal y las partes manifestarán en sus respectivos escritos de calificación las pruebas de que intenten valerse, presentando listas de peritos y testigos que hayan de declarar a su instancia». En otras palabras, la tónica habitual es que la prueba se proponga y aporte en los escritos de calificación, esto es, al acabar la fase de instrucción. Pero, hay una salvedad, pues en el procedimiento abreviado, que se regula en los artículos 757 y ss. de la L.E.Crim., la preclusión anterior no se aplica, extendiéndose hasta el momento del juicio oral[47]. En cualquier caso, es conveniente manifestar los medios de prueba tras la redacción de las conclusiones provisionales, esto es, en el escrito de calificación no tiene que solicitarse que se acrediten los medios de prueba que se quieran practicar mediante la fórmula *otrosí*, sino tras la redacción de las conclusiones y antes del suplico.

Ya tenemos respondidos el cómo y el cuándo se ha de aportar la prueba electrónica al proceso penal, y lo cierto es que se cumple con la regla general. Sin embargo, el Legislador ha sido previsor al tener en cuenta la volatilidad de los futuros medios de prueba, de ahí que tengamos que analizar la regulación supletoria que se recoge en los artículos 297 y siguientes de la L.E.C. Así pues, con el objetivo de asegurar las pruebas propuestas, permite que «antes de la iniciación de cualquier proceso, el que pretenda incoarlo o cualquiera de los litigantes durante el curso del mismo, podrá pedir del tribunal la adopción, mediante providencia, de medidas de aseguramiento útiles para evitar que, por conductas humanas o acontecimientos naturales, que puedan destruir o alterar objetos materiales o estados de cosas, resulte imposible en su momento practicar una prueba relevante o incluso carezca de sentido proponerla». Podemos entonces certificar que, al tratarse de pruebas volátiles, el Legislador ha querido que se aseguren en el tiempo, hasta tal punto de que se puede solicitar la copia de lo contenido en los dispositivos tecnológicos, incluido el teléfono móvil.

Además, cabe destacar que la Ley Orgánica 13/2015, la cual reformó la Ley de Enjuiciamiento Criminal, introdujo el artículo 588 *octies*, en el cual se otorga tanto al Ministerio Fiscal como a la Policía Judicial el poder para requerir a cualquier persona física en la conservación de datos o informaciones concretas contenidos en un sistema de almacenamiento informático[48]. Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días. Es más, el propietario de ese sistema informático estará

[47] Véase artículo 785 de la L.E.Crim.

[48] **Artículo 588 octies Orden de conservación de datos**: «El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes. Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días. El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado 3 del artículo 588 ter e».

obligado a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, estará obligado a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

Por último, decir que se ha contemplado la posibilidad de aplicar las funciones criptográficas *hash*[49], ya que permiten cifrar una entrada de datos en un dispositivo, dando como resultado salidas de mayor o menor longitud dependiendo de cómo fuera la entrada de datos. Así pues, esta técnica «consiste en hacer una copia espejo de un disco duro, memoria USB, un CD o, incluso, un teléfono móvil. Las dificultades de la realización de esta copia dependerán de los múltiples entresijos de los dispositivos mencionados»[50]. Se entiende, en este sentido, que medidas de aseguramiento tradicionales como el depósito no son suficientes para garantizar la integridad de los datos almacenados, de ahí que se acuda al empleo de estas funciones matemáticas. En cambio, no basta hacerse con los *hashes*, sino que es necesaria la ulterior protocolización notarial del original, previa imagen o copia espejo de un teléfono móvil[51]. Entonces, si se aplican bien estas funciones se pueden resolver problemas relacionados con la volatilidad y manipulación de la mensajería instantánea.

Pese a ello, se han desarrollado otras formas, esta vez *online,* de certificación y custodia de las pruebas electrónicas. En este sentido, uno de los sistemas más conocidos es el de *DOYFE.ES* (www.doyfe.es), pues permite certificar el contenido de una página web concreta, de una imagen alojada en un dispositivo o, incluso, de un correo electrónico alojado en cualquier servidor de Internet. En todo caso, conviene advertir que no es un sistema que permita ofrecer una total seguridad jurídica, ya que se limita exclusivamente a cristalizar y dar por verificada una página web, una imagen o un correo electrónico, sin resolver si tales fueron previamente manipulados. Por tanto, si empleamos este tipo de sellados de tiempo, los problemas de autoría y de manipulación de la prueba electrónica seguirían estando intactos. Del mismo modo, resulta inaudito considerar que hoy en día nuestros Tribunales de Justicia den por válidas este tipo de certificaciones digitales, tanto por el desconocimiento de las mismas como por el hecho de que no se conozcan las garantías que este tipo de herramientas pueden ofrecer al proceso penal[52]. Se trata, entonces, de una cuestión de futuro.

---

[49] Por *hash* se entiende aquel «algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor *hash* de salida tendrá siempre la misma longitud». Más información en https://blog.kaspersky.com.mx/que-es-un-hash-y-como-funciona/2806/

[50] PEREIRA PUIGVER, S.: «Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte», *Fodertics II: Hacia una justicia 2.0. Estudios Sobre Derechos y Nuevas Tecnologías*, Ed. Ratio Legis, Salamanca, 2014, pág. 79.

[51] PEREIRA PUIGVERT, S.: *La exhibición de… op*., cit, págs. 90 y ss.

[52] Más información en http://www.audea.com/es/herramientas/certificacion-y-acta-de-prueba-electronica/

3. *De las formas de proposición y aportación de la prueba electrónica y su eficacia: del «pantallazo» al uso del «hash»*

En la práctica profesional, los operadores jurídicos se encuentran con multitud de formas de incorporar al proceso la prueba electrónica; pero, no de todas se desprende la misma eficacia. En palabras de DELGADO MARTÍN, la multiplicidad de los instrumentos y elementos tecnológicos determina una heterogeneidad de las formas de acceder a su contenido[53]. Así, el punto de partida lo establece el artículo 299 de la L.E.C., y es que según entendamos la naturaleza jurídica de la prueba electrónica, así serán los medios a través de los cuales esta se puede incorporar al proceso. Si consideramos, en primer lugar, que a la prueba electrónica se le aplica el apartado primero, pues podrá incorporarse al proceso penal bien como prueba documental, bien como pericial, bien como reconocimiento judicial[54], o bien como interrogatorio de los acusados o testigos.

En cambio, si consideramos que a la prueba electrónica se le aplica el artículo 299.2, pues esta podrá acceder al proceso a través de los instrumentos tecnológicos que permiten la «reproducción de la palabra, el sonido y la imagen» o aquellos que permitan «archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

Por último, se le puede aplicar el apartado tercero, y es que «por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias».

Así las cosas, tenemos que admitir que se puede hacer un uso amplio de los medios que recoge el artículo 299 de la L.E.C., ya que se admite el uso de cualquiera de ellos, siempre y cuando respeten los principios de unidad, comunidad, contradicción, ineficacia, inmediación, oportunidad y oralidad de la prueba. Sin embargo, una cosa es que se permita el uso de un abanico amplio de medios, y otra muy diferente es que de su incorporación al proceso se desprenda una mayor o menor eficacia jurídica. En este sentido, es habitual encontrarnos con prácticas profesionales como la impresión de los mensajes enviados por *WhatsApp* o la aportación de los denominados «pantallazos».

[53] DELGADO MARTÍN, J.: *La prueba electrónica… op*., cit, págs. 3 y 4.

[54] En este orden de cosas, podemos plantear lo siguiente: ¿el artículo 353 de la L.E.C. ofrece la cobertura jurídica necesaria como para realizar un ciberrastreo judicial? Es más, ¿cuentan los Jueces con los conocimientos/aptitudes suficientes así como con los recursos informáticos necesarios como para reconocer judicialmente los dispositivos móviles incautados a un investigado? ALONSO-CUEVILLAS SAYROL ha llegado a afirmar que esta posibilidad de reconocimiento judicial al espacio virtual puede ser un medio idóneo para llevar al proceso información fáctica contenida en ella. Y es que, respecto de la red, puede terminar siendo útil, necesario o conveniente el uso del reconocimiento judicial. Véase, en este sentido, ALONSO-CUEVILLAS SAYROL, J.: «Internet y prueba civil», *Revista Jurídica de Cataluña*, Vol. 100, núm. 4 Barcelona, 2011, pág. 286.

Pues bien, este tipo de prácticas no suelen ser nada eficaces, ya que se obvian datos especialmente importantes como son la autoría y la autenticidad de los mensajes aportados. Por tanto, es importante dejar constancia de la integridad de los mensajes, y eso se consigue con el mero análisis del almacenamiento original de la información (basta con presentarse el teléfono móvil, *tablet* u otro dispositivo en el que se hayan recibido esos mensajes), y el posterior cotejo pericial del terminal.

Con ello, se analizarán uno a uno los medios más utilizados en la práctica jurídica, poniendo especial atención a su eficacia:

- **Trascripción privada del mensaje en un documento**: consiste en realizar una simple impresión en soporte documental (en papel) de aquello que se encuentra alojado electrónicamente en un dispositivo de almacenamiento (como es el caso del teléfono móvil). Esta es una práctica que habitualmente desempeñan los distintos operadores jurídicos, pero que ve su eficacia jurídica reducida en caso de ser impugnada. Es más, es habitual aportar en el proceso civil este tipo de transcripciones escritas, mediante las cuales se intenta demostrar la existencia de una deuda económica y el posterior reconocimiento de la misma en una conversación de *WhatsApp*. Así pues, este tipo de prácticas si tienen cabida en el proceso civil; ya que, en caso de no ser impugnadas (artículos 326.1 y 319 de la L.E.C.), se podría otorgar valor probatorio a esa conversación de *WhatsApp* que se aporta para el reconocimiento de una deuda[55]. En cambio, en el proceso penal concurren intereses de carácter público, de ahí que normalmente se impugne la trascripción escrita, pues se obvian datos tan importantes como la autoría de los mensajes de *WhatsApp* transcritos en un documento. Por consiguiente, esta técnica no es conveniente en el proceso penal, y su eficacia es mínima al tratarse de un medio volátil y fácilmente manipulable.
- **Aportación de capturas de pantalla**: esta técnica es una derivación de la anterior, y consiste en aportar en soporte documental capturas de pantallas o «pantallazos» de las conversaciones que intentan probarse en el proceso. Sin embargo, en el proceso penal se trata de proteger, entre otras, la presunción de inocencia, y esta técnica en muchas ocasiones la destruye al dar por auténticos mensajes de *WhatsApp* que fácilmente han podido ser manipulados. Así las cosas, el Tribunal Supremo, consciente de que estos dispositivos son volátiles, se ha encargado de establecer unos requisitos a la hora de otorgar valor probatorio a este tipo de conversaciones. En este sentido, la Sentencia de la Sala Segunda del Tribunal Supremo número 300/2015, de 19 de mayo, estableció 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

[55] Véase Sentencia de la Audiencia Provincial de Alicante número 4/2014, de 9 de enero.

fin, la integridad de su contenido»[56]. Por tanto, esta técnica otorgará valor probatorio a esas capturas de pantalla, siempre y cuando se certifique la autoría y la autenticidad de las conversaciones. En otras palabras, esta técnica en sí misma tiene poca eficacia jurídica, pues necesita del aparejamiento de una prueba pericial informática y de la aportación del sistema original de almacenamiento de la información del teléfono móvil.

- **Levantamiento de acta por el Letrado de la Administración de Justicia**: si las anteriores técnicas consiguen ofrecer poca eficacia jurídica, esta aún todavía brinda menos. Consiste en la intervención en calidad de fedatario público del Letrado de la Administración de Justicia con el objetivo de que corrobore que la trascripción de los mensajes recibidos en los dispositivos de almacenamiento móvil se asemeja con los mensajes originales, y que tanto el dispositivo y los números de teléfono corresponden con los aportados. Sin embargo, esta técnica no otorga en sí eficacia a la prueba presentada, pues el Letrado de la Administración de Justicia no certifica ni la autoría de los mensajes ni la autenticidad de los mismos, sino que únicamente da fe de lo que ve. Así, esta técnica tampoco es capaz de acabar con el problema de la manipulación de las conversaciones mantenidas en aplicaciones de mensajería instantánea.

  Sin embargo, esta técnica fue admitida en Sentencia de la Audiencia Provincial de Córdoba número 159/2014, de 2 de abril, ya que «según consta en la diligencia extendida por el mismo el 20 de diciembre de 2.013 (folio 44), procediera a la "trascripción xerográfica de los mensajes recibidos por doña Dolores [nombre ficticio] en el terminal número NUM003". Por tanto, del propio texto de la diligencia resulta que quien ostentaba la fe pública judicial, ejercitada dentro del marco de lo dispuesto en el artículo 453 de la Ley Orgánica del Poder Judicial, con carácter exclusivo y pleno, dejó constancia de un hecho con trascendencia procesal. Nada hay que objetar a un acto consistente en reflejar, merced a una serie de fotocopias de las diversas pantallas del terminal presentado por la denunciante, determinados mensajes a través de *WhatsApp* asociados a un usuario con nombre "José Miguel" [nombre ficticio], el del denunciado, incorporadas a los autos entre los folios 46 y 78». Sin embargo, esta técnica logró otorgar valor probatorio a los mensajes de *WhatsApp* pues su autoría fue reconocida en juicio por el acusado (F.J. º2)[57]. Se hizo, pues, una valoración global de las pruebas aportadas y practicadas en el juicio oral.

- **Aportación de acta notarial/protocolización notarial**: al igual que la anterior, esta técnica tampoco ofrece una eficacia jurídica suficiente como para otorgar valor probatorio a las conversaciones aportadas; pues, de nuevo, el Notario en calidad de fedatario corrobora que la aportación de la trascripción de los

[56] http://www.poderjudicial.es/stfls/SALA%20DE%20PRENSA/NOTAS%20DE%20PRENSA/TSPenal%2027.11.15%20(10333-15).pdf

[57] http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7100605&links=&optimize=20140619&publicinterface=true

mensajes recibidos, del dispositivo móvil y de los números de teléfono se asemeja con originales. Tampoco, es capaz de solucionar el problema de la volatilidad de esta *app*[58].

- **Prueba de interrogatorio de las partes o prueba testifical**: en este caso, se intenta acreditar la autenticidad de la prueba electrónica mediante el reconocimiento expreso del acusado del envío de las conversaciones aportadas en el proceso. Esta técnica, aunque afectada por el derecho a no declarar, otorgó completo valor probatorio a los mensajes de *WhatsApp* en la Sentencia de la Audiencia Provincial de Córdoba número 159/2014, de 2 de abril. En este sentido, «el propio acusado ha llegado a reconocer en el acto del juicio (a la altura aproximada del minuto 7:45 de la grabación) haber remitido uno de los mensajes de "Whatsapp" cuya autoría le atribuye el relato de hechos probados, ya que admitió que por dicho medio le dijo a la denunciante que iba a matar a su novio (la expresión que figura en la imagen, folio 47, es "pos lo voi a reventar delante tuya")» (F.J. º2).

- **Prueba pericial informática**: esta técnica consiste en analizar el dispositivo del teléfono móvil, con el objetivo de conocer si se produjo alteración o manipulación (autenticidad e integridad) de los mensajes de *WhatsApp*. Se trata así de emitir «un dictamen sobre los hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos»[59]. Por tanto, como se dijo anteriormente, es necesario preservar la integridad de los dispositivos de almacenamiento originales, pues es la única forma segura de saber si los mensajes fueron o no alterados. En este sentido, la Sentencia de la Audiencia Provincial de Madrid número 51/2013, de 23 de septiembre, entendió que al no existir «otro medio de prueba que avale la declaración del acusado […]» ni al practicar «sobre los mismos prueba pericial informática que acredite su autenticidad y su envío por aquél» no se podía estimar el recurso de apelación interpuesto por una víctima de violencia de género que intentaba dejar sin efecto la Sentencia de primera instancia.

- **Reconocimiento judicial:** consiste en el examen directo del Juez del dispositivo tecnológico en el que se encuentran almacenadas las conversaciones de *WhatsApp* (artículo 353 de la L.E.C). De nuevo, sería necesario acudir a la prueba pericial informática para demostrar la autenticidad e integridad de aquello que fue aportado.

[58] Véanse artículos 199 y ss. del Decreto 2 junio 1944, *por el que se aprueba con carácter definitivo el Reglamento de la organización y régimen del Notariado.*

[59] Siguiendo la tesis planteada en http://ala.org.es/la-validez-probatoria-del-whatsapp-y-su-incorporacion-al-procedimiento/

- **Aportación como medio audiovisual (imágenes, sonidos o palabras captadas por medios de filmación, grabación o semejantes**): si entendemos que la prueba electrónica se trata de un instrumento que permite la «reproducción de la palabra, el sonido y la imagen», se puede entregar al Juzgado cualquier imagen, grabación o sonido que permita demostrar la realización de una actividad ilícita. Pues bien, en este supuesto se entregaría al Juzgado esa imagen, grabación o sonido mediante su copia en un CD, DVD o USB. De igual forma, esta aportación tendría que ir acompaña de trascripción escrita, y de nuevo tendría poca eficacia pues necesitaría de prueba pericial informática para demostrar la autenticidad e integridad de aquello que fue aportado.

- **Empleo de herramientas que permiten dejar «huella digital»**: como se expuso con anterioridad, existen nuevos medios para certificar la integridad y autenticidad de las conversaciones que fueron aportadas en el proceso. Uno de los más estudiados ha sido el uso de las funciones criptográficas *hash*, pues permiten hacer una copia espejo de un disco duro, memoria USB, un CD o, incluso, un teléfono móvil. Sin embargo, para darle mayor eficacia, es necesaria la ulterior protocolización notarial del original, previa imagen o copia espejo del teléfono móvil[60]. Así pues, si se aplican bien estas funciones se pueden resolver problemas relacionados con la volatilidad y manipulación de la mensajería instantánea. En todo caso, no todos los tipos de *hash* desprenden la misma eficacia, pues derivaciones como «MD5» o «Algoritmo de Firma de Mensajes 5» (a pesar de ser el más usado) es cuestionada por los peritos informáticos, dando mayor credibilidad a *hashes* como «SHA-256» y «SHA-1»[61].

  También, se ha desarrollado el Sistema/Autoridad de Sellado de Tiempo «TSA - Time Stamp Authority», a través del cual se prueba que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos fue modificado desde entonces. En otras palabras, permite «probar la existencia de un documento electrónico, su transmisión o recepción por un sistema externo, etc. […], se generará una evidencia, que determinará la existencia de ese documento en un instante determinado»[62]. En cambio, este sistema ha sido mucho menos utilizado en la práctica profesional, ya que, a pesar de tener su cobertura jurídica en la Ley 59/2003, de 19 de diciembre, *de firma electrónica* y en la Ley 11/2007, de 22 de junio, *de acceso electrónico de los ciudadanos a los Servicios Públicos*, se aplica para probar la existencia de documentos electrónicos en general.

Resumiendo, los Tribunales han entendido que debe otorgarse valor probatorio a los mensajes de *WhatsApp* aportados cuando nos encontremos en:

[60] PEREIRA PUIGVERT, S.: *La exhibición de… op.*, cit, págs. 90 y ss.

[61] Véase, en este sentido, http://www.genbeta.com/movil/whatsapp-envia-sus-mensajes-encriptados-pero-su-seguridad-sigue-siendo-baja

[62] Siguiendo la tesis planteada en https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/notario

- Los supuestos de no impugnación: en el sentido de lo dispuesto en la Sentencia de la Audiencia Provincial de Alicante número 4/2014, de 9 de enero.
- Los supuestos de reconocimiento expreso: en el sentido de lo dispuesto en la Sentencia de la Audiencia Provincial de Córdoba número 159/2014, de 2 de abril.
- En caso de cotejo del otro terminal afectado: en este sentido, la Sentencia de la Audiencia Provincial de Barcelona número 143/2014 de 7 de mayo.
- En caso de impugnación y si existe prueba pericial informática: véase, Sentencia de la Audiencia Provincial de Madrid número 51/2013, de 23 de septiembre.

Sin embargo, junto a los medios anteriormente descritos, la L.E.Crim. otorga poderes tanto a la Policía Judicial (artículo 282) como al Juez de Instrucción (artículo 326.1.º) para hacerse con aquellos dispositivos electrónicos que hayan de ser utilizados como medio de prueba en un proceso penal por contener información relevante para la acreditación de los elementos y circunstancias del delito[63].

Y esa aprehensión de los dispositivos se hará bajo la responsabilidad del Letrado de la Administración de Justicia (artículo 338). También, la L.E.Crim. permite el registro de cualquier sistema informático que se encuentre en un lugar cerrado. Así, para acceder a ellos hará falta de una diligencia de entrada y registro (artículos 573 y ss.). En este sentido, la Sentencia del Tribunal Supremo número 785/2008, de 25 de noviembre, que resuelve un supuesto de posesión y difusión de pornografía infantil afirma que «la policía estaba autorizada a recoger los objetos o instrumentos de los que pudiera deducirse la comisión del delito y que fueran hallados en el recinto registrado, y en este sentido se intervienen los ordenadores y su disco duro».

Finalmente, la L.E.Crim. permite el registro remoto o registro *online* en sus artículos 350 y siguientes. Así pues, mediante el uso de «troyanos»[64] se accede al contenido de un sistema informático sin necesidad de proceder a la aprehensión física del dispositivo electrónico. Se trata, entonces, de acceder al sistema informático (ordenador, teléfono móvil, *tablet*, etc.) mediante la instalación de un troyano para escanear todas las unidades de almacenamiento y remitir de forma remota y automatizada el contenido del mismo al informático de la autoridad responsable de la investigación[65]. La reforma de la L.E.Crim. permite así el uso de *spyware*[66] o *malware*[67] para obtener prueba electrónica.

[63] DELGADO MARTÍN, J.: *La prueba electrónica… op*., cit, págs.. 4 y ss.

[64] Por «troyano» podemos entender una clase de virus informático que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.) con el objeto de infectar y causar daño. Así, son capaces de capturar y reenviar datos confidenciales a una dirección externa o abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota. Más información en http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/

[65] DELGADO MARTÍN, J.: *La prueba electrónica… op*., cit, pág.. 8 y ss.

IV. ADMISIÓN, PRÁCTICA Y VALORACIÓN DE LA PRUEBA ELECTRÓNICA EN EL ORDEN JURISDICCIONAL PENAL

1. *Admisión y práctica de la prueba electrónica*

Como se expuso con anterioridad, nuestro Ordenamiento admite distintas formas de incorporar la prueba electrónica al proceso penal. En este sentido, la regla general es que la prueba electrónica viene a admitirse y practicarse; y no solo eso sino que se le otorga completo valor probatorio en el orden jurisdiccional penal, siempre y cuando se trate de averiguar hechos de relevancia jurídica, la prueba sea pertinente y se respeten los derechos fundamentales, así como la integridad de lo aportado. Dicho esto, tenemos que acudir al Título III del Libro III de la L.E.Crim. para analizar la práctica de la prueba electrónica durante el juicio oral. Pues bien, si la prueba electrónica fue incorporada al proceso como prueba de interrogatorio del investigado o de la víctima tendremos que acudir a los artículos 688 y ss. de la L.E.Crim., mientras que si lo fue como prueba testifical se aplicarán los artículos 701 y ss. Por el contrario, si se incorporó como prueba pericial se aplicarán los artículos 723 a 725; o, finalmente, como prueba documental, los artículos 726 y 727.

Así, el momento oportuno para practicarse las diligencias de prueba reguladas en los artículos 688 a 727 será el del juicio oral, donde se respetarán los principios de inmediación, igualdad de condiciones, contradicción y publicidad. Por tanto, en esta fase se practicarán todas las pruebas propuestas y aportadas en los escritos de calificación, siempre y cuando fueran admitidas y pudieran ser practicadas; lo que provocará que se concreten las peticiones tanto de la acusación (o acusaciones) como de la defensa.

Pues bien, en primer lugar, respecto de la práctica del interrogatorio del acusado, decir que se comenzará interrogando a este sobre sus datos personales y, a continuación, se le requerirá para que manifieste si se declara culpable o inocente del delito por el que se le investiga. Si reconociera los hechos objeto de investigación, esto es, que aceptara ser el autor de la conversación de *WhatsApp* aportada o del envío de grabaciones, imágenes o sonidos constitutivos de delito, se otorgará valor probatorio a lo reconocido y se dará por finalizada la práctica de la prueba (véase, en este sentido, la Sentencia de la Audiencia Provincial de Córdoba número 159/2014, de 2 de abril).

Por el contrario, en caso de que haya falta de conformidad de los acusados con la acusación o en caso de tratarse de un delito para cuyo castigo se haya pedido pena aflictiva (las de mayor gravedad), se practicarán las testifícales propuestas en los

---

[66] El *spyware* consiste en la instalación de un *software* espía, teniendo como objetivo principal hacerse con los datos almacenados en un dispositivo informático así como espiar los movimientos que se realizan por la red. Para ello, actúa en *background* o en segundo plano. Más información en https://www.infospyware.com/articulos/que-son-los-spywares/

[67] Por el contrario, el *malware* es un tipo de *software* malicioso que trata de infectar un ordenador, un teléfono o una *tablet*, con el pretexto de extraer información personal. Más información en https://www.avast.com/es-es/c-malware

escritos de calificación. Así las cosas, se dará lectura a los escritos de calificación y a las listas de peritos y testigos que se hubiesen presentado oportunamente, haciendo relación de las pruebas propuestas y admitidas. Después, se pasará a la práctica de las diligencias de prueba y al examen de los testigos, empezando por la que hubiere ofrecido el Ministerio Fiscal, continuando con la propuesta por los demás actores, y, por último, con la de los procesados. Además, las pruebas de cada parte se practicarán según el orden con que hayan sido propuestas en el escrito correspondiente.

En tercer lugar, se practicarán los informes periciales si existiese su proposición, y los peritos que no hayan sido recusados serán examinados juntos cuando deban declarar sobre unos mismos hechos y contestarán a las preguntas y repreguntas que las partes les dirijan. Por tanto, estos podrán ser recusados por las causas y en la forma descrita en los artículos 468, 469 y 470 de la L.E.Crim. Entonces, si la prueba pericial informática consigue determinar la autoría y la integridad de los dispositivos de almacenamiento originales, se le otorgará valor probatorio a los mensajes de *WhatsApp* aportados y se condenará al autor por los hechos objeto de investigación (véase, en este sentido, la Sentencia de la Audiencia Provincial de Madrid número 51/2013, de 23 de septiembre). Finalmente, si la prueba electrónica se incorpora al proceso como documental, el Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad. En otras palabras, es práctica habitual que las documentales se den por reproducidas con los escritos de calificación, pues ya fueron examinadas previamente por el Tribunal.

Pese a ello, la L.E.Crim. en su artículo 730 estipula que «podrán también leerse o reproducirse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral, y las declaraciones recibidas de conformidad con lo dispuesto en el artículo 448 durante la fase de investigación a las víctimas menores de edad y a las víctimas con discapacidad necesitadas de especial protección». Por consiguiente, si se aportasen medios audiovisuales, tales como imágenes, sonidos o palabras captadas por medios de filmación, grabación o semejantes, se reproducirán durante el juicio oral. Sin embargo, si las partes disponen de una copia de la grabación o de la trascripción escrita no es necesaria su reproducción en juicio –o al menos no de todo el contenido–, debiendo limitarse a aquellos pasajes o extremos de su interés. También, el artículo 729.2º de la L.E.Crim. permite que se practiquen las diligencias de prueba no propuestas por ninguna de las partes, que el Tribunal considere necesarias para la comprobación de cualquiera de los hechos que hayan sido objeto de los escritos de calificación.

Finalmente, también se admite la práctica de pruebas anticipadas, ya que la L.E.Crim. ha entendido que, en caso de que no puedan practicarse durante el juicio oral, se practicarán antes de ese momento procesal dado que, por ejemplo, puede desaparecer la información contenida en los dispositivos de almacenamiento (véanse los artículos 448 y ss. de la L.E.Crim). Esto permite que la prueba electrónica sea

analizada con autenticidad e integridad, y respetando las garantías constitucionales básicas. Del mismo modo, se podría llegar a admitir la práctica de pruebas preconstituidas, y es que, por ejemplo, durante un cacheo rutinario los agentes de la autoridad podrían haber descubierto el envío de numerosos mensajes de *WhatsApp* en los cuales se extorsiona a un empresario para que pague una cantidad determinada de dinero, pues en caso contrario su local de negocio será destruido. Ante estos casos, lo normal es que se proceda a la incautación *in situ* del dispositivo móvil.

2. *¿WhatsApp, prueba válida?: Análisis de los últimos pronunciamientos judiciales*

Como sabemos, y hemos indicado con anterioridad, no existe en nuestro Ordenamiento una regulación específica para este tipo de medio probatorio, de ahí que la tarea de adaptar el Derecho a los cambios sociales le haya correspondido a la jurisprudencia. Y juega aquí una baza muy importante la L.E.Crim. pues en su artículo 741 afirma que «el Tribunal, apreciando, según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley». Así, todo dependerá de una valoración del Juez conforme a las normas de la sana crítica, las máximas de la experiencia y los conocimientos científicos aceptados. Se trata de una libre apreciación/valoración, pero con los límites legalmente establecidos: la apreciación no puede ser equivocada, absurda o irracional, entre otras cosas porque libre valoración no equivale a libre arbitrio, de ahí la exigencia constitucional de motivación de las decisiones judiciales.

En este sentido, se abordarán los pronunciamientos que los Tribunales de Justicia españoles han emitido en los últimos años, donde los mayores problemas que se han desarrollado han sido la fácil manipulación de las conversaciones y la gran dificultad de probar la autoría de las mismas. Por consiguiente, la jurisprudencia no es unánime a la hora de resolver, de ahí que nos encontramos ante sentencias discordantes en su argumentación y en su fallo, pues algunas otorgan valor probatorio a los mensajes de *WhatsApp*, mientras que otros pronunciamientos no aceptan la validez de los mismos alegando problemas de autoría y manipulación. Pese a ello, la regla general es el otorgamiento de valor probatorio a las conversaciones de *WhatsApp*. Analicemos, así, los pronunciamientos judiciales con mayor relevancia práctica –por orden cronológico– que se han dictado en el orden jurisdiccional penal:

- La **Sentencia número 1260/2012, de 1 octubre, de la Audiencia Provincial de Madrid** fue uno de los primeros pronunciamientos judiciales que abordó la problemática de la manipulación de los mensajes de *WhatsApp*. Resolviendo un delito contra la salud pública por tráfico de sustancia estupefaciente de los artículos 368 y 369.5ª. del Código Penal, la Audiencia Provincial de Madrid dio por válidos los «pantallazos» del teléfono móvil de uno de los acusados que fueron acompañados por el Equipo de Policía Judicial de la Jefatura del Servicio Fiscal y Aeroportuario de la Guardia Civil. La defensa, por el contrario, entendía que debía declararse «la nulidad del contenido de todas las transcripciones unidas a las actuaciones así como de los "pantallazos" del teléfono móvil del acusado»,

ya que se había producido «una injerencia ilegítima por parte de los agentes actuantes con vulneración del artículo 18.3 de la Constitución» (F.J. 1º).

Así pues, en un supuesto de interceptación de las comunicaciones, la Audiencia entendió que «la injerencia […], previa autorización judicial, es legítima y por lo tanto, sin vulneración "ilegítima" de los derechos fundamentales, por lo que no cabe apreciar causa de nulidad», de ahí que «todos elementos probatorios son válidos, lícitos y legítimos, susceptibles de plena valoración a la hora de enjuiciar los hechos objeto de acusación» (F.J. 1º *in fine*). Es más, dio por probados los hechos, siendo «legalmente constitutivos de un delito contra la salud pública previsto y penado en el artículo 368 del Código Penal por tráfico de drogas y penado en el artículo 369.1.5ª. por lo de notoria importancia» (F.J. 2º).

- Por otro lado, el **Auto del Tribunal Supremo de 14 de febrero de 2013**, en el que se inadmite el recurso de casación formalizado contra la anterior Sentencia de la Audiencia Provincial de Madrid, acuerda mantener el fallo de la misma, pues considera que este sistema de mensajería instantánea es un medio válido para acreditar determinados hechos. En este sentido, «el acceso por parte de los agentes de la Guardia Civil al contenido de las aplicaciones del teléfono móvil de XXX, accediendo así al contenido de las conversaciones mantenidas entre dicha persona y el contacto "XXX", mediante la aplicación *WhatsApp*, afecta al derecho constitucional al secreto de las comunicaciones protegido en el artículo 18.3 de la CE, si bien la misma se lleva a cabo previa autorización judicial mediante auto de fecha 29 de septiembre de 2011».

  Es más, «en dicho Auto se da autorización al equipo de Policía Judicial para que pueda encender el terminal telefónico intervenido a XXX, al objeto de comprobar y reseñar datos sobre las comunicaciones existentes vía SMS, vía MMS, vía *WhatsApp*, y datos de contacto de la agenda. Por lo tanto, la injerencia en esa comunicación es legítima y no se ha vulnerado ningún derecho fundamental, por lo que no cabe apreciar causa de nulidad. […] Partiendo de esa base, no puede alegarse que se haya vulnerado el derecho al secreto de las comunicaciones» (F.J. 6º *in fine*). En conclusión, la intervención de las conversaciones mantenidas en *WhatsApp* requiere «las mismas exigencias que la intervención de cualesquiera otras comunicaciones, fundamentalmente, una resolución judicial motivada, ponderando los intereses en juego y respetando la debida proporcionalidad entre la utilidad y pertinencia de la prueba con la afectación a los derechos fundamentales de la personas afectada»[68].

- Del mismo modo, esta vez en un supuesto de violencia de género, la **Sentencia 12/2013, de 5 abril, de la Audiencia Provincial de Madrid** otorga valor probatorio a los mensajes enviados a través de *WhatsApp* que se transcribieron en el Juzgado de Violencia Sobre la Mujer número 3 de Madrid. Se acreditó, así pues, la autenticidad de esos mensajes mediante la prueba testifical que se

[68] Siguiendo la tesis planteada en http://ceaj.es/i-premio-monografico-2016-nulidad-de-la-prueba-por-vulneracion-del-art-18-4-ce-por-carlos-donoro-ayuso/

propuso y practicó junto a las documentales consistentes en la trascripción de las conversaciones mantenidas en esta *app*. En otras palabras, la Audiencia entendió que al no existir «otro medio de prueba que avale la declaración del acusado […]» y al no practicarse «sobre los mismos prueba pericial informática que acredite su autenticidad y su envío por aquél» no se podía estimar el recurso de apelación interpuesto por el condenado.

Es más, la Audiencia estipula que «los mensajes, enviados a través del *WhatsApp*, que han resultado transcritos en el Juzgado de Violencia Sobre la Mujer nº 3 de Madrid, al inicio de las actuaciones judiciales que, como ya anticipábamos, adquieren un singular valor probatorio, porque, tanto por la secuencia horaria en que las comunicaciones entre XXX y XXX se realizan, como por el contenido de las mismas, suponen un elemento de corroboración objetiva puntual y exacta de lo declarado, coincidentemente, por las dos testigos». Finalmente, la Audiencia otorga valor probatorio a las conversaciones de *WhatsApp* aportadas en el proceso, pues junto a esa trascripción de mensajería se acompañó prueba testifical que corroboraba el contenido exacto y objetivo de los mensajes.

- También, la **Sentencia número 1396/2013 de la Audiencia Provincial de Barcelona, de 7 de noviembre** concede valor probatorio a las conversaciones de *WhatsApp* aportadas, ya que «la versión de los hechos ofrecida […] ha quedado plenamente corroborada por el contenido de los mensajes remitidos vía *WhatsApp* desde el móvil del recurrente al móvil de la Sra. Lucía [nombre ficticio] que desde luego no consta haya sido manipulado, que se recogen en el acta de exhibición […] que resultan suficientemente explícitos y merecedores de reproche penal» (F.J. 1º *in fine*).

  Así pues, admite la integridad de los mensajes de *WhatsApp* aportados al proceso, ya que su trascripción se puso en consonancia con el resto de las pruebas practicadas. Esto es, al hacerse una valoración conjunta del material probatorio**,** **«**se acepta el relato de hechos probados de la Sentencia apelada que se expresa en los siguientes términos: "Único. Se considera probado que sobre las 15:18 horas del día 11 de noviembre de 2011, Aníbal [nombre ficticio] envió desde su teléfono móvil un *WhatsApp* al móvil de su ex pareja Lucía en el que con ánimo de amedrentarla le decía: "*la estás cagando pero bien cagada. Así que tu misma. Si eres tan chula para no hablarme e ir de malota luego no llores por mi te lo juro eli. Que al final uno de los dos acabamos muertos. Asi que no me toques la polla. Y hablame cuanto mas rato te tires pasando de mi mas te voy a joder la vida" lo que causo un gran temor a esta"*» (Hechos Probados).

  Con ello, se desestima el recurso de apelación interpuesto por el acusado, ratificándose la resolución en los siguientes extremos: «debo condenar y condeno a Aníbal como autor penalmente responsable de un delito de amenazas en al ámbito familiar de menor entidad sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de dieciséis días de

Trabajos en Beneficio de la Comunidad, privación especial para el derecho a la tenencia y porte de armas por seis meses y un día y prohibición de aproximarse en una distancia inferior a 1000 metros a la persona de Lucía a su domicilio, lugar de trabajo y cualquier otro en el que se encontrara y de comunicarse con ella por cualquier medio por un periodo de un año» (Antecedente de Hecho Primero).

- Sin embargo, la **Sentencia 10/2014, de 10 enero, de la Audiencia Provincial de Pontevedra** se pronuncia acerca de la insuficiencia en la determinación de la titularidad del teléfono desde el que se vertieron vejaciones y ofensas al denunciante. Pues bien, aparte de la existencia y colocación de numerosos carteles y del envío de numerosos *WhatsApp*, cuyo contenido era puramente vejatorio y ofensivo, no se otorga valor probatorio al medio de prueba aportado pues, unido a que las declaraciones de los testigos no son concluyentes, se desconoce la titularidad real del teléfono desde el que se envían los mensajes. En otras palabras, la Audiencia Provincial de Pontevedra determina que «la prueba que sustenta la condena del recurrente, aparte del dato objetivo de la existencia de los carteles y *WhatsApp*, de indiscutible carácter vejatorio y ofensivo, se deriva de las manifestaciones de la denunciante, pues no consta siquiera la titularidad del teléfono desde el que se envían los mensajes y las declaraciones de los testigos no son concluyentes. Tales datos, se estima, son manifiestamente insuficientes para deducir de ellos, con el nivel de certeza necesario para sustentar una Sentencia condenatoria».

  Por consiguiente, la Audiencia aborda la problemática de la autoría de los de los mensajes de *WhatsApp*, y es que es consciente de que, no existiendo prueba pericial que corrobore la autoría de los mismos, no se pueden dar por válidos mensajes que son fácilmente manipulables. Así, existiendo impugnación de la prueba documental aportada, no se puede dejar constancia ni de la titularidad del terminal desde el que se enviaron los mensajes, aún más cuando las testificales que se practicaron no vertieron constancia puntual y exacta de lo aportado. Entonces, la única forma real y objetiva de demostrar la titularidad de las vejaciones y ofensas vertidas a través de *WhatsApp* es con la práctica de una prueba pericial informática.

- En el mismo sentido, la **Sentencia 31/2014, de 28 enero, de la Audiencia Provincial de Cádiz** no otorga valor probatorio a los mensajes enviados a través de *WhatsApp*, «pues no habiendo declarado los dos implicados, de la existencia de lesiones no puede desprenderse el origen de su autoría y unos mensajes de *WhatsApp* sobre los que ningún técnico ha declarado y que no consta que sean veraces o emitidos por el apelante o que no hayan podido ser manipulados, no es suficiente prueba para sustentar en ella el pronunciamiento condenatorio que se combate, razón que hace procedente la estimación del recurso».

  En otras palabras, de este pronunciamiento puede dilucidarse la importancia de que un técnico informático haga constar la veracidad de los mensajes de *WhatsApp*, pues en todo momento debe acreditarse no solo la existencia de una

conversación entre dos o más personas, sino la remisión y posterior recepción de la misma por los destinatarios. Y ello se hará a través del cotejo de la información y de la averiguación de la titularidad real de los terminales. En conclusión, debido a la facilidad de manipulación de la prueba electrónica y a la falta de proposición de interrogatorio de las partes, la intervención de un perito informático para elaborar el correspondiente dictamen pericial puede ser muchas veces necesaria y hasta determinante (artículo 335 de la L.E.C.)[69].

- La **Sentencia número 159/2014 de la Audiencia Provincial de Córdoba, de 2 de abril**, en un supuesto de levantamiento de acta por parte del Letrado de la Administración de Justicia, otorga valor probatorio a los mensajes de *WhatsApp* transcritos, ya que «según consta en la diligencia extendida por el mismo el 20 de diciembre de 2.013 (folio 44), procediera a la "trascripción xerográfica de los mensajes recibidos por doña Dolores [nombre ficticio] en el terminal número NUM003". Por tanto, del propio texto de la diligencia resulta que quien ostentaba la fe pública judicial, ejercitada dentro del marco de lo dispuesto en el artículo 453 de la Ley Orgánica del Poder Judicial, con carácter exclusivo y pleno, dejó constancia de un hecho con trascendencia procesal. Nada hay que objetar a un acto consistente en reflejar, merced a una serie de fotocopias de las diversas pantallas del terminal presentado por la denunciante, determinados mensajes a través de *WhatsApp* asociados a un usuario con nombre "José Miguel" [nombre ficticio], el del denunciado, incorporadas a los autos entre los folios 46 y 78» (F.J. 2º).

  Así, este modo de aportar la prueba electrónica al proceso logró otorgar valor probatorio a los mensajes de *WhatsApp* pues su autoría fue reconocida en juicio por el acusado (F.J. 2º *in fine*). Sin embargo, tal y como se anunció con anterioridad, esta técnica no otorga en sí eficacia a la prueba presentada, pues el Letrado de la Administración de Justicia no certifica ni la autoría de los mensajes ni la autenticidad de los mismos, sino que únicamente da fe de lo que ve. Por tanto, esta técnica necesita, para conseguir acabar con el problema de la manipulación de las conversaciones mantenidas en aplicaciones de mensajería instantánea, de la práctica de otras pruebas, como por ejemplo del interrogatorio del acusado.

  Es más, el F.J. 2º *in fine* de la Sentencia reconoce que «la trascendencia probatoria del documento no depende tan solo de su contenido, sino del crédito que merece al juzgador lo declarado por la Sra. Dolores, puesto que, al fin y al cabo, de lo que se trata es de su relato, que no solo está corroborado por lo que en la diligencia de constancia figura, sino por la confirmación de su autenticidad que, aun de manera parcial, pero harto significativa, le otorga el reconocimiento efectuado por el acusado de que, efectivamente, le remitió mensajes a través de dicho medio de comunicación, mensajes intrínsecamente intimidatorios,

[69] OLIVA LEÓN, R. (Coord.) y otros: «La prueba electrónica envenenada», *La prueba electrónica: validez y eficacia procesa*l, Colección Desafíos Legales #RetoJCF, Juristas con Futuro, 2016, pág. 59.

concordes con lo denunciado. Mal podría decretarse la nulidad de una diligencia que, además, no irroga indefensión alguna, ya que se ha podido discutir con plenitud su trascendencia, sin que la ausencia de Letrado en el momento de levantarla haya restado posibilidad alguna a la representación del Sr. José Miguel».

- Del mismo modo, la **Sentencia número 533/2014 de la Audiencia Provincial de Madrid, de 24 de julio** desestima el recurso de apelación presentado contra la Sentencia del Juzgado de Violencia sobre la Mujer nº 1 de Alcorcón dictada el día 19 de noviembre de 2013, en el que «se condena a Eduardo [nombre ficticio] como autor responsable de una falta de injurias prevista y penada en el artículo 620.2º, último párrafo del Código Penal, a la pena de seis días de localización permanente» (Antecedente de Hecho Primero). Y es que «resultado probado y así se declara expresamente que el día 28-05-13, María Antonieta vio en el estado de la aplicación *WhatsApp* del número de teléfono de Eduardo, que el mismo había puesto el texto siguiente: "*Mi ex María Antonieta es una mental enferma, tonta, una mentirosa y una mala madre. Denuncia que no va a ningún sitio niñata!!!*"» (Antecedente de Hecho Primero). Así, la presente Sentencia es uno de los pronunciamientos pioneros que resuelve una falta de injurias (con la nueva regulación, delito leve) que se lleva a cabo a través del estado de *WhatsApp*.

  Es más, afirma que «es obvio el contenido injurioso y vejatorio de la expresiones que el denunciado recogía en el estado de su *WhatsApp* y, aunque el mismo manifieste que no todos ellos iban dirigidos a la denunciante, sino también a sus familiares y amigos, es obvio que cualquier persona que tuviera en su lista de contactos el teléfono móvil del denunciado podía ver el estado de *WhatsApp* del mismo y las injurias que dirigía a su ex pareja sentimental, siendo las expresiones que se recogían en dichos estados obviamente injuriosas y dirigidas a vejar, humillar y molestar a la madre de su hijo, siendo las mismas incardinales en el artículo 620.2 del Código Penal por el cual fue condenado el recurrente, lo cual nos conduce a la desestimación del recurso y a la confirmación de la resolución recurrida» (F.J. 3º *in fine*).

  Por tanto, no se castiga al autor del estado de *WhatsApp* por el hecho exclusivo de vejar y humillar a la víctima, sino que es plenamente consciente de que el estado de *WhatsApp* actúa como medio de propagación de fotos, vídeos o información.

- La **Sentencia de la Sala Segunda del Tribunal Supremo número 300/2015, de 19 de mayo**, se ha convertido en uno de los pronunciamientos más importantes en lo que se refiere a la impugnación de la autenticidad de las conversaciones mantenidas en aplicaciones de mensajería instantánea. En primer lugar, el Tribunal Supremo desplaza la carga de la prueba a quien pretende aprovecharse de ella, esto es, «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» (F.J. 4º *in fine*).

A mayores, el Tribunal establece criterios para la eficacia probatoria de los «pantallazos», y es que «las conversaciones mantenidas entre Ana María e Constancio [nombres ficticios], incorporadas a la causa mediante "*pantallazos"* obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada *a posteriori* para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional. Así lo ha declarado de forma reiterada esta Sala en relación, por ejemplo, con las transcripciones de diálogos o conversaciones mantenidas por teléfono, por más que consten en un soporte escrito o incluso sonoro (por todas, SSTS 956/2013 de 17 diciembre ; 1024/2007 , 1157/2000, 18 de julio y 942/2000, 2 de junio)» (F.J. 2º).

En otras palabras, el Tribunal Supremo es consciente de que la prueba electrónica encaja dentro del contenido del apartado tercero del artículo 299 de la L.E.C., de ahí que, si se impugna la trascripción de una conversación o los «pantallazos» realizados a la misma, ello no tiene validez alguna, pues hay que cuestionar el soporte original de almacenamiento de las conversaciones. En cualquier caso, esta valoración no queda exenta de polémica, pues muchos autores siguen considerando que la conversación que queda registrada en un soporte informático es un documento, digital, pero al final y al cabo un documento.

Finalmente, estipula 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» (F.J. 4º *in fine*).

Por tanto, a la técnica de las capturas de pantalla se le otorgará valor probatorio siempre y cuando se certifique la autoría y la autenticidad de las conversaciones. En otras palabras, el Tribunal Supremo, consciente de la fácil manipulación de las conversaciones de *WhatsApp* y de la difícil determinación de la autoría de las mismas, ofrece poca eficacia a la técnica del «pantallazo», pues claramente tiene que ir acompañada de la práctica de una prueba pericial informática o de la aportación del sistema original de almacenamiento de la información del teléfono móvil. Así y a falta de su reconocimiento expreso por la otra parte, será necesario un informe pericial que identifique el teléfono emisor de los mensajes delictivos, o una prueba testifical que acredite su remisión.

Tras haberse publicado esta Sentencia, una de las cuestiones que mayor problemática ha suscitado ha sido la de la privatización del proceso. En este sentido, muchos autores advierten lo que significa que el Tribunal Supremo dé prioridad a la práctica de prueba pericial informática y además desplace la carga de la prueba hacia quien pretende valerse de ella. Pues bien, es recomendable que, teniendo en cuenta los bienes jurídicos que están en juego, sea el mismo órgano jurisdiccional el que de oficio mande efectuar la pericial informática valiéndose de los funcionarios públicos especializados en la materia. Es recomendable, entonces, exigir de oficio la práctica de prueba pericial informática, pues de realizarse a instancia de parte colisionaría con la capacidad económica de la víctima y se vulneraría el artículo 24.1 de la Constitución Española al no obtenerse una tutela judicial efectiva.

- Por otra parte, **la Sentencia número 89/2015 de la Audiencia Provincial de Zaragoza, de fecha 17 de septiembre,** desestima el recurso de apelación interpuesto contra la Sentencia del Juzgado de Instrucción nº 1 de Zaragoza, de fecha 27 de abril de 2015, en la que se condena a María Virtudes [nombre ficticio] como autora criminalmente responsable de una falta de coacciones a la pena de 6 días de localización permanente. Y ello porque se dan por probados numerosos estados de *WhatsApp* constitutivos de una falta de coacciones. Así las cosas, en el Fundamento Jurídico Tercero de la Sentencia se estipula que «el llamado estado de *WhatsApp*, es simplemente eso, el contenido del mismo en un determinado momento y al que tienen acceso las personas que en aquel grupo participan. Por lo tanto, los argumentos de la recurrente intentando explicar algo tan banal como lo es que no se trata de mensajes o correos, carecen de toda consistencia, pues al tener acceso a su contenido todas las personas integrantes del grupo y que se supone que acceden al mismo con frecuencia (de lo contrario carecería de sentido la formación de tales grupos o sus miembros se borrarían del mismo) es obvio que quien inserta un nuevo comentario, noticia, video, foto o cualquier otro material lo hace para que los demás miembros tengan acceso al mismo».

  Con ello, la Audiencia Provincial de Zaragoza deja claro que todo comentario, noticia, vídeo, foto o cualquier otro material que se inserta en el estado de *WhatsApp* puede ser constitutivo de delito, sobre todo cuando «las explicaciones dadas por la recurrente en el acto de la vista en el sentido de que se trataba de "casualidades" son del todo inverisímiles e increíbles y ello ante la evidencia de que a través de los estados de *WhatsApp* se estaban transmitiendo situaciones a tiempo real, y no en una sino en cuatro concretas ocasiones tal y como de los hechos probados se desprende» (F.J. 3º *in fine*).

- También, la **Sentencia de 30 de diciembre de 2015 (Recurso 896/2013) del Juzgado de Primera Instancia e Instrucción número 1 de Moncada (Valencia)** otorga valor probatorio al condenar a un médico por intromisión ilegítima al honor, en el sentido de reparar en su estado de *WhatsApp* el honor de su antiguo socio, después de que hubiera mantenido en su estado de *WhatsApp*

desde el 23 de mayo hasta el 17 de septiembre de 2013 la frase «No te fíes de Javier Gutiérrez» [nombre ficticio]. Es más, el condenado tuvo que pagar a su ex socio 2.000 euros de indemnización. Lo más característico de este pronunciamiento mediático es que el condenado tuvo que mantener en su estado de *WhatsApp* durante 60 días la siguiente rectificación: «Mediante sentencia de fecha 30-12-2015, J.M. [nombre ficticio] fue condenado por intromisión ilegítima en el honor de Javier Gutiérrez».

En cualquier caso, poco es lo que diferencia esta resolución a las anteriores, ya que se resuelve de una manera muy similar la eficacia probatoria de los estados de *WhatsApp*. En cambio, la clave estuvo en que no resultó hecho controvertido que los citados hechos se produjeran «en un contexto de desavenencias personales y empresariales entre los litigantes, que provocaron diversas acciones judiciales entre ellos» ni «tampoco se discute que el citado mensaje estuvo visible en el estado de la cuenta de *WhatsApp* del demandado desde el 23 de mayo de 2013 hasta el 17 de septiembre de 2013, como queda acreditado también con las actas notariales aportadas» (F.J. 1º). Esto es, no hay impugnación del estado de *WhatsApp* transcrito, de ahí que únicamente la resolución analice el alcance del artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, *sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

- De la misma manera, la **Sentencia 189/2016, de 13 de mayo, de la Audiencia Provincial de Burgos** otorga valor probatorio a la prueba electrónica aportada, ya que condenó a los acusados como autores de un delito de revelación de secretos, imponiendo una pena de prisión de un año para cada uno de ellos, así como una indemnización por daños morales con importe total de 3.000 euros. La Audiencia Provincial de Burgos estima el recurso de apelación interpuesto por la víctima contra la Sentencia desestimatoria procedente del Juzgado de lo Penal nº 1 de Burgos. De este modo, queda probado que «Demetrio [nombre ficticio] tenía en su poder una fotografía de su ex pareja, Sabina [nombre ficticio], en la que esta aparecía sin la parte superior del bañador, cubriendo con sus manos los pechos» (Antecedente de Hecho Primero). Dicha fotografía fue publicada como foto de perfil de *WhatsApp* por parte de Elisa [nombre ficticio], actual pareja del acusado, siendo manipulada con una especie de viñeta con las letras «WOW». Posteriormente, la imagen aparecía con el siguiente texto «*Quien juega con fuego…arde!!! (y todavía hay 100 más)*».

  Uno de los mayores problemas fue conocer cómo la fotografía había llegado a manos del acusado, de ahí que la Sentencia de primera instancia reconociera la atipicidad de la conducta imputada, ya que ni los acusados habían «accedido, alterado o utilizado datos de carácter personal o familiar de Sabina que se encuentren recogidos en un fichero de datos» ni esa fotografía «constituye un dato de carácter personal, médico, académico o económico que se encuentre en un fichero de datos ya sea público o privado» (F.J. 3º).

Finalmente, la Audiencia procedió a estimar el recurso de apelación interpuesto reconociendo que «no cabe duda de que el teléfono móvil personal es un soporte informático donde consta un registro de archivos de carácter personal, que está protegido por la LO 15/1.999 de Protección de los Datos de carácter Personal, y por el art. 197.2 introducido por la LO 15/2.003, que reformó el CP introducido por la LO 10/1.995, y ha mantenido la reforma operada por la LO 5/2.010, y ampliado por la LO 1/ 2.015, que en su párrafo 3º ya regula de forma específica "la difusión, revelación o cesión a terceros de datos o hechos descubiertos o las imagines captadas a que se refieren los dos párrafos anteriores"» (F.J. 3 *in fine*).

- Por otra parte, la **Sentencia 98/2016, de 16 de junio, del Juzgado de lo Penal de Teruel** condenó a quince meses de prisión y multa de quince meses con cuota diaria de seis euros a un joven por un delito contra la intimidad por descubrimiento y revelación de secretos, y a 9 meses de prisión por un delito contra la integridad moral. En este sentido, fue condenado por grabar con el móvil imágenes sexuales de una menor y difundirlas después por *WhatsApp* entre su grupo de amigos. Así, resultó probado que «en la madrugada del día 1 de enero de 2013, sobre las 07,30 horas el acusado en esta causa SANTIAGO ISRAEL A. G. [nombre ficticio], mayor de edad y sin antecedentes penales, se trasladó en su vehículo desde la Plaza Bolamar de Teruel hasta el barrio de La Fuenfresca en compañía de la denunciante "A" y de su amigo Joaquín T. A. [nombre ficticio]; llegados a este lugar detuvo la marcha del turismo y los tres jóvenes decidieron entablar relaciones sexuales, materializadas en una felación que "A" realizó simultáneamente a los dos varones en el asiento trasero. Sin conocimiento ni consentimiento de "A", el acusado tomó dos fotografías de la escena en la que aparece nítidamente el rostro de la denunciante, realizando las instantáneas con la cámara de su teléfono móvil marca *iPhone* teniendo abierta la aplicación de *WhatsApp* del grupo "pon un reloj en tu vida" al que pertenecía el acusado junto a su amigo Joaquín T., entre otros, difundiéndola acto seguido entre los miembros del *chat* a las 07:37:36 horas» (Hechos Probados).

  Es más, «en el mes de junio de ese año, en concreto el día 3, a través de *WhatsApp* se produjo la difusión masiva […], principalmente entre los jóvenes, de las dos fotografías de contenido sexual que hacen referencia a "A", las cuales habían sido rotuladas con comentarios sarcásticos e hirientes, acompañadas de una fotografía de su perfil en la red social *Tuenti*, creando este hecho gran impacto emocional en la víctima que ha visto cuestionada su conducta en términos despectivos y ha sido sometida al escarnio público» (Hechos Probados *in fine*). Así las cosas, SANTIAGO ISRAEL fue condenado como autor de un delito de descubrimiento y revelación de secretos del artículo 197.1 del Código Penal y de un delito contra la integridad moral del 173.1 del Código Penal, siendo absuelto de un delito de corrupción de menores del artículo 189.1 b).

  Se realizó, de esta forma, informe pericial emitido por el Grupo de Informática Forense, dependiente de la Unidad Central de Criminalística de la Comisaría General de Policía Científica, basado en la resolución judicial que autoriza el

volcado de las conversaciones de *WhatsApp* de varios teléfonos móviles, y se concluye que el acusado envió las imágenes en la fecha expuesta. A raíz de la práctica del informe pericial, la Defensa puso en duda el valor de la trascripción efectuada por Policía Científica a la luz de la Sentencia del Tribunal Supremo, de fecha 26 de mayo de 2015, pero se le otorgó finalmente valor probatorio a la trascripción pues el contenido fue corroborado por prueba testifical (F.J. 1º *in fine*).

Por consiguiente, quedó «probado que el acusado realizó dos fotografías de la denunciante en el momento y lugar indicado en los hechos declarados probados, el cual se ha de calificar de íntimo ya que es notorio que las cuestiones relativas a la vida sexual de la persona constituyen parte del núcleo del concepto de intimidad, como "ámbito propio y reservado frente a la acción y el conocimiento de los demás"» (F.J. 2º). Es más, «no medió consentimiento de la perjudicada para la obtención de las imágenes posteriormente difundidas», pues «no hubo por parte de la víctima una declaración de voluntad expresa ni en sentido positivo ni en sentido negativo» (F.J. 2º).

- Finalmente, la **Sentencia 50/2016, de 20 de junio, del Juzgado de Violencia sobre la Mujer número 1 de Granada** concede valor probatorio al intercambio de mensajes de *WhatsApp*, hasta el punto de que condenó a su autor por mandar «a la mierda» a su pareja mediante este medio de mensajería instantánea. Fue condenado por un delito leve de injurias/vejaciones en el ámbito familiar, previsto y penado en el artículo 173.4 del Código Penal; lo que se traduce en cinco días de localización permanente en domicilio diferente y alejado al de la víctima. En todo caso, la Sentencia concluye que, atendiendo a las circunstancias en las que se produce el delito, resulta adecuado imponer la pena anterior, por ser la mínima prevista para este delito leve.

  La resolución admite la concurrencia de los siguientes elementos: «a) Uno de carácter objetivo, comprensivo de las acciones o expresiones que lesionan la dignidad de la persona, menoscabando su fama o atentando contra su propia estimación. b) Otro de índole subjetiva, acusadamente intencional, en cuanto que aquellas frases o actitudes han de responder al propósito específico de ofender, vilipendiar, desacreditar, vejar, menospreciar, escarnecer, etc. a la persona destinataria de ellas o a la que vienen referidas, *animus iniuriandi*, en suma, que representa el elemento subjetivo del injusto y que soporta la infracción injuriosa. c) El tercer elemento, complejo y circunstancial, aglutina cuantos factores o datos personales, de ocasión, lugar, tiempo, forma, etc., (la naturaleza, efectos y circunstancias a que hace referencia nuestro Código) que valorativamente apreciados contribuyan, de una parte, a esclarecer la verdadera intención o propósito que animaba al sujeto proferidor de la ofensa, y, de otra, coadyuven a determinar la importancia y magnitud de la misma».

  Resulta así acreditado que el acusado, con intención de ofender a su pareja sentimental, le envió un mensaje vía *WhatsApp* en el que le decía «*vete a la*

mierda». Finalmente, los hechos fueron reconocidos por el acusado, dictándose así Sentencia de conformidad, gozando ya de plena firmeza y sin necesidad de celebrarse vista oral dentro del juicio rápido por delito leve.

Expuestos los pronunciamientos judiciales con mayor importancia práctica que se han dictado en el orden jurisdiccional penal, lo cierto es que la regla general se sitúa en otorgar valor probatorio a los mensajes de *WhatsApp* aportados. En los últimos años, los Tribunales de Justicia españoles han sido conscientes de la importancia que ha adquirido la prueba electrónica y, en especial, las conversaciones de *WhatsApp* a la hora de intentar probar hechos judiciales controvertidos. Sin embargo, los Tribunales no han admitido *de facto* o automáticamente la validez de este tipo de mensajería, sino que la han sometido a rigurosas y necesarias limitaciones. Son, por tanto, plenamente conscientes de la fácil manipulación de estos sistemas, aún más cuando no se puede demostrar la persona concreta que envió dicha información constitutiva de delito (ya sean imágenes, videos o grabaciones), poniéndose en riesgo la presunción de inocencia amparada por el artículo 24 de nuestra Carta Magna.

Así, es conveniente contestar a la siguiente pregunta: ¿hasta qué punto puede una conversación de *WhatsApp* servir como prueba en un juicio? Pues bien, dada la volatilidad de estos nuevos medios de prueba, la práctica habitual de los Tribunales es hacer una valoración global de todo el material probatorio presentado. En otras palabras, dará por válidos e íntegros los mensajes de *WhatsApp* siempre y cuando del interrogatorio del acusado o de las testificales practicadas se demuestre que el contenido de las conversaciones es efectivamente el transcrito. Además, el Tribunal Supremo –en Sentencia número 300/2015, de 19 de mayo–es plenamente consciente de este problema, de ahí que haya desplazado la carga de la prueba a quien pretende aprovecharse de la prueba electrónica, dejando sentado que la prueba pericial informática será indispensable a la hora de identificar el verdadero origen de esa comunicación, la identidad de los interlocutores y la integridad de su contenido (F.J. 4º *in fine*).

En cambio, el rango de validez de los *WhatsApp* como prueba en un juicio va ligado a la técnica mediante la cual se han aportado al proceso. Así, prácticas habituales como la trascripción privada, la aportación de los «pantallazos» o la entrega de USBs, tarjetas de almacenamiento y similares son poco eficaces a la hora de demostrar hechos controvertidos, pues ni demuestran la autoría de lo enviado ni la integridad de su contenido. Por tanto, los Tribunales se han visto obligados a dar cobertura jurídica a la prueba electrónica a través de la práctica de pruebas de interrogatorio de las partes, de pruebas testifícales y, sobre todo, a través de pruebas periciales informáticas.

En conclusión, lo más importante es acabar con la lacra de la vulnerabilidad de estas *app*, asegurando el empleo de pruebas periciales informáticas y adaptando nuestro Ordenamiento a las Nuevas Tecnologías. Y, aquí, es dónde cobra especial relevancia el hecho de tener una regulación sólida, neutral y específica que acabe con esta problemática y avance hacia una *Justicia 2.0*.

V. DE LA AUTENTICIDAD Y COTEJO DE LA PRUEBA ELECTRÓNICA

1. *La vulnerabilidad de las aplicaciones de mensajería instantánea: su fácil manipulación*

A lo largo de este Trabajo Fin de Título, se han puesto de manifiesto las vulnerabilidades que sufre actualmente *WhatsApp*; las cuales también resultan extensibles al resto de las aplicaciones de mensajería instantánea. Pues bien, el riesgo evidente de manipulación de estos medios de prueba, unido a la imposibilidad de conocer la autoría real de las conversaciones, ha provocado que sea práctica habitual recurrir a la impugnación procesal de las pruebas propuestas y aportadas en los escritos de calificación (tanto de la/s acusación/es como de la defensa). Entonces, resulta necesario realizar una valoración global de todas las pruebas presentadas en el proceso judicial, pues en sí la aportación de una conversación transcrita de *WhatsApp* –o de los «pantallazos» de la misma– no logra aproximarse hacia la autenticidad e integridad de la prueba electrónica.

Esta situación se ha intentado mitigar en abril de 2016 por parte de la compañía *WhatsApp* con la activación del cifrado «E2EE» («end-to-end»). Lo que viene a significar este cifrado es que los mensajes, fotos y vídeos que envíen los usuarios de la aplicación estarán cifrados «de extremo a extremo», o sea, esto equivaldría a que emisor y receptor serán los únicos que podrán tener acceso a las conversaciones que entre ellos han mantenido. Sin embargo, esto tampoco ha conseguido acabar con las vulnerabilidades de la aplicación, aún más cuando los propios proveedores de Telecomunicaciones no pueden acceder a los mismos (contraviniéndose, en cierto modo, el deber de colaboración que se recoge en el artículo 588 *ter* e de la L.E.Crim.). La activación de este cifrado ya ha provocado, por ejemplo, que no se entregue a los investigadores del «Caso Diana Quer» las últimas conversaciones que mantuvo la joven antes de su desaparición, pues por parte de la compañía se alega posible incumplimiento de las políticas de privacidad[70].

Así las cosas, lo cierto es que la prueba electrónica tiene una serie de caracteres que la hacen la *rara avis* de entre los distintos medios de prueba que se admiten en nuestro Ordenamiento. Hagamos, pues, referencia sucintamente a cada uno de ellos[71]:

- En primer lugar, **se trata de una prueba de fácil reproducción**: lo que viene a significar que fácilmente puede trascribirse el contenido de la misma. Así, es habitual realizar copias de las distintas conversaciones que se han mantenido a través de *WhatsApp*, siendo posteriormente propuestas y aportadas en un proceso judicial concreto. En cambio, en muy pocos casos se acompaña el original junto con esas copias.

[70] Siguiendo la tesis planteada en http://www.elconfidencial.com/espana/2016-10-25/whatsapp-diana-quer-guardia-civil_1279664/

[71] Siguiendo la tesis mantenida en GÓMEZ DEL CASTILLO Y GÓMEZ, M.: «Aproximación a los nuevos medios de prueba en el proceso civil», *Revista Derecho y conocimiento de la Facultad de Derecho de la Universidad de Huelva*, Vol. I, 2001, págs. 5-12.

- Además, **resulta ser una prueba volátil**: como se ha expresado con anterioridad, las pruebas electrónicas son fácilmente manipulables, esto es, pueden ser modificadas con facilidad; tanto es así que se puede alterar el contexto de las conversaciones o, incluso, cambiar por completo la redacción de los distintos mensajes. Una de las técnicas más usadas para alterar los *WhatsApp* es descargando la base de datos de la aplicación que almacena nuestro terminal al obtenerse los permisos de *root*[72], almacenar dicha información en un ordenador y, posteriormente, mediante un comando mostrar una lista con todos los archivos almacenados para después modificarlos con programas accesibles al público, como «SQLiteStudio»[73]. Hasta tal punto la aplicación es alterable que, en el año 2014, se estimaba que el 40% de los *WhatsApp* aportados en juicio eran falsos[74].

- Del mismo modo, **la prueba electrónica puede ser fácilmente destruida**: *WhatsApp* no sólo puede ser manipulado, sino que las bases de datos que se almacenan en los distintos dispositivos móviles pueden ser borradas, incluso se ha llegado hasta el extremo de destruir los almacenamientos originales de información (o sea, los móviles). Aquí, la expresión «sin cuerpo no hay delito» se actualizaría al mundo 2.0, dando lugar la expresión «sin móvil no hay delito».

- En ocasiones, **resulta un medio intrusivo a la hora de obtener información**: como bien se expresó con anterioridad, la prueba electrónica puede haber sido obtenida de forma ilícita, esto es, se pueden haber puesto en riesgo los derechos fundamentales que se consagran en nuestra Constitución. Existe, entonces, un margen muy estrecho entre la obtención lícita y la obtención ilícita de este tipo de mensajería instantánea, y conviene baremar las colisiones de los distintos derechos fundamentales. Para ello, la citada Circular 1/2013 de la Fiscalía General del Estado ha establecido algunas pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. En cambio, no solo debe protegerse el derecho al secreto de las comunicaciones, sino otros tan importantes como el derecho a la intimidad personal y la autodeterminación informativa, el derecho a la inviolabilidad domiciliaria o el derecho a la protección de datos de carácter personal.

Por el contrario, lo cierto es que nos encontramos ante evidencias electrónicas que, a diferencia de las tradicionales, dejan huella (digital), a pesar de haber sido modificadas, borradas o destruidas. Y aquí es donde cobra vital importancia el informe que un perito informático pueda realizar sobra la materia. Pero, el juzgador

[72] Por *root* entendemos el acceso a un dispositivo móvil con los permisos de «superusario», esto es, con los privilegios que ofrece el fabricante del *hardware* del *smartphone*, *tablet* u otro dispositivo. Con este acceso, se tendrá la capacidad de reemplazar las distintas aplicaciones del sistema, sus configuraciones, o ejecutar *software* especializado que de otra forma es inaccesible. Más información en https://hipertextual.com/archivo/2014/01/acceso-root-android/

[73] http://www.redeszone.net/2015/10/02/asi-se-pueden-falsificar-los-mensajes-de-whatsapp/

[74] «El 40% de los 'whatsApps' y SMS usados en juicios son falsos, según la Asociación de Internautas», *Diario Público*, 22 de agosto de 2014 [consultado el 4 de noviembre de 2016].

no se puede quedar ahí, sino que tiene que tener en cuenta la diferencia dogmática existente entre autenticidad e integridad de la prueba electrónica. En este orden de cosas, DELGADO MARTÍN[75] entiende que autenticidad es aquella «coincidencia de su autor aparente con su autor real». O sea, se trata de una «característica consistente en que se garantice la autenticidad del origen de los datos, es decir, la fuente de la que proceden los datos». En cambio, por integridad de la prueba electrónica entiende aquella «propiedad o característica consistente en que los datos (activo de información) no han sido alterados de manera no autorizada».

En definitiva, la primera va vinculada a la aplicación del principio de libre valoración de la prueba por el juez o de las reglas de la sana crítica, ya que para determinar la autenticidad de la prueba normalmente es necesario realizar una valoración conjunta de todos los elementos probatorios (por ejemplo, hay que poner en relación la trascripción de una conversación de *WhatsApp* con las distintas pruebas testificales que se practican durante la vista oral); mientras que la integridad trata de garantizar la cadena de custodia o preservación de los datos. Y esta diferenciación terminológica es importante en la práctica cuando se impugnan pruebas de carácter electrónico.

2. Formas de autenticación: la necesaria práctica de prueba pericial informática

Quizá el mayor problema con el que se encuentran los distintos operadores jurídicos es el de la inexistencia de base de datos externas donde se almacenan las conversaciones mantenidas por un usuario a través de *WhatsApp*. En este sentido, *WhatsApp* –y el resto de aplicaciones de mensajería instantánea– funciona de una manera muy distinta a como lo hacen las multinacionales *Facebook*, *Twitter* o *Instagram*. Así, estas últimas almacenan en bases de datos externas millones de imágenes, videos, conversaciones, etc., y tienen la obligación de conservarlas por un determinado periodo de tiempo. Sin embargo, *WhatsApp* no cuenta con ellas, pues en sí la información que se transmite queda almacenada en el dispositivo en el que se encuentre instalada la aplicación.

En cualquier caso, la L.E.Crim. ha previsto de forma parcial esta dificultad, pues en su artículo 588 *ter* k, establece que «cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en Internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión de algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 *ter* e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso».

[75] DELGADO MARTÍN, J.: «La prueba del WhatsApp», *Diario La Ley*, nº 8605, Sección Tribuna, Ed. LA LEY, 2015, pág. 6.

Así, los proveedores de Telecomunicaciones y de Internet estarán obligados a colaborar con la Justicia y entregar aquellos datos que permitan identificar y localizar al sospechoso de cometer un hecho delictivo, así como al terminal desde el cual se desarrollaron las distintas actividades. En cualquier caso, la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* limita esta potestad hasta el punto de que «los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial» (artículo 6) siempre que «sean requeridos […] con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales» (artículo 1).

La existencia de estas limitaciones, agravadas aún más con las nuevas políticas de privacidad de *WhatsApp* y la activación del cifrado «de extremo a extremo», viene a dar como resultado que sean pocos los métodos a través de los cuales se puede autentificar y verificar la originalidad de aquellas conversaciones que se aportan en juicio. En este sentido, son muchos los que creen conveniente el uso de las funciones criptográficas *hash*, con el objetivo de demostrar que un mensaje fue manipulado, borrado o destruido. En cambio, si entendemos que estas funciones matemáticas permiten cifrar una entrada de datos en un dispositivo dando como resultado salidas de mayor o menor longitud dependiendo de cómo fuera la entrada de datos, en sí este análisis no nos arroja el contenido exacto del mensaje que se ha cifrado. En otras palabras, mediante el empleo de estas técnicas no se consigue verificar objetivamente el contenido del mensaje, pues básicamente su empleo tiene como resultado una cadena de números y letras que no se asemejan a lo que entendemos por lenguaje legible; y que cambiaría de longitud y caracteres de ser modificado el mensaje. Por tanto, el uso del *hash* es satisfactorio siempre y cuando sea empleado como técnica de aseguramiento de la prueba electrónica, y no como método que permita demostrar la autenticidad y originalidad de una conversación. Lo mismo ocurre con la aplicación del Sistema de Sellado de Tiempo TSA - *Time Stamp Authority*.

Así las cosas, la única técnica judicial que hoy en día existe para demostrar que un *WhatsApp* fue alterado es la práctica de una prueba pericial informática. De esta manera, el punto de partida lo constituye el artículo 335.1 de la L.E.C., pues establece que «cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal». Pues bien, nuestro Ordenamiento da cabida a la práctica de pruebas periciales con el objetivo de adquirir certeza sobre hechos controvertidos con trascendencia jurídica. Es más, el artículo 352 de la L.E.C. establece, en relación con la admisión de los nuevos medios de prueba fruto del apartado tercero del artículo 299, que «cuando sea necesario o conveniente para conocer el contenido o sentido de una prueba o para proceder a su más acertada valoración, podrán las partes aportar o proponer dictámenes periciales

sobre otros medios de prueba admitidos por el tribunal al amparo de lo previsto en los apartados 2 y 3 del artículo 299».

Por tanto, al reconocerse expresamente la emisión de dictámenes periciales, esta técnica tiene una eficacia mucho mayor que la que tienen técnicas como los «pantallazos» o las testifícales. Conscientes de esta eficacia, los operadores jurídicos se centran en cuestionar si los conocimientos del técnico encargado de hacer un peritaje son los suficientes como para demostrar objetivamente la autenticidad de una evidencia electrónica. En cambio, desvirtuar una prueba informática es extremadamente difícil, dada su laboriosidad y especialización. En cualquier caso, es sabido que los peritos informáticos poseen amplios conocimientos en lo que se refiere a las Nuevas Tecnologías, siendo indispensable «poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este» (artículo 340.1 de la L.E.C.) o «solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia» (artículo 340.2 de la L.E.C.).

Así, esa acreditación profesional es suficiente para ejercer como perito en los Juzgados y Tribunales españoles. Es más, es aplicable el contenido recogido en la Instrucción número 5/2001, de 19 de diciembre de 2001, del Pleno del Consejo General del Poder Judicial *sobre remisión anual a los órganos jurisdiccionales de listas de profesionales para su designación judicial como peritos*, así como en el Acuerdo de 28 de octubre de 2010, del Pleno del Consejo General del Poder Judicial, *por el que se modifica la Instrucción 5/2001, de 19 de diciembre, del Consejo, sobre remisión anual a los órganos jurisdiccionales de las listas profesionales para su designación judicial como peritos y del Protocolo de actuación del servicio común procesal para la asignación de peritos judiciales, de 9 de febrero de 2005*. Y, aquí, lo importante para los operadores jurídicos es conocer que «cuando haya de designarse perito a persona sin título oficial […] se realizará la designación […] usándose para ello una lista de personas que cada año se solicitará de sindicatos, asociaciones y entidades apropiadas, y que deberá estar integrada por al menos cinco de aquellas personas» (Apartado Primero del Acuerdo). Por tanto, desvirtuar la falta de conocimientos de un profesional en la pericia informática no es cuestión sencilla.

En otro orden de cosas y para que la práctica de una prueba pericial informática sea aceptada por los Tribunales de Justicia españoles, es recomendable analizar el soporte original de almacenamiento de la información, esto es, es necesario analizar tanto el teléfono móvil desde el que se han enviado esas conversaciones como el terminal en el que se han recibido. Por tanto, y al igual que ocurre con la impugnación judicial de los correos electrónicos, es necesario dejar a un lado las copias de las conversaciones mantenidas por *WhatsApp* que se hayan reproducido, así como del resto de transcripciones y capturas de pantalla. Así mismo, es requisito *sine qua non* preservar y garantizar la cadena de custodia, pues desde la obtención de la prueba hasta el análisis de autenticidad puede pasar un largo periodo de tiempo.

Es recomendable, de esta forma, conservar la prueba en la forma protocolariamente prevista. Y, esta exigencia la marca la Sentencia del Tribunal Constitucional de 29 de septiembre de 2003 pues establece ciertas pautas que deben cumplirse en el supuesto de que algo se incaute, pues de lo contrario la prueba pericial sería ilícita por vulneración de las garantías constitucionales básicas. Es necesario, entonces, que se describan los materiales incautados en la Diligencia del Letrado de la Administración de Justicia (véase, artículo 334 de la L.E.Crim.) o, en caso de no haber requerimiento judicial, mediante la copia y depósito ante Notario. Y, después, es necesario que la prueba se conserve y analice conforme a lo establecido en los distintos protocolos de actuación que tienen las Fuerzas y Cuerpos de Seguridad del Estado. Por ello, es práctica habitual que se impugne la prueba por la mala praxis de los protocolos.

Así, con fecha de 31 de mayo de 2011 se aprobó el Manual del Servicio de Policía Judicial de la Guardia Civil en el que se recoge en el Apartado 4.9 la forma de intervención de las comunicaciones; normativa que se desarrolla en el Manual de Orientaciones para la Práctica de Diligencias por la Policía Judicial de 24 de febrero de 2016. Entre otras exigencias, la Policía Judicial verá su campo de actuación limitado al tener que seguir escrupulosamente con lo ordenado por la autorización judicial que permite la interceptación, siendo el ámbito de actuaciones centralizado hacia los órganos designados por el Ministerio del Interior, o sea, el Sistema de Integrado de Interceptación Telefónica (más conocido como S.I.T.E.L.) será el encargado de interceptar las comunicaciones.

Del mismo modo, se recoge la forma de proceder en la solicitud de información a los proveedores de Telecomunicaciones e Internet, ya que se prevé que la intervención podrá «afectar a los terminales o medios de comunicación de los que sea titular o usuario, habitual u ocasionalmente, el investigado». También, la Ley Orgánica 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* permite a S.I.T.E.L. intervenir las comunicaciones telefónicas y telemáticas «por el tiempo estrictamente necesario para la realización de las averiguaciones tendentes al esclarecimiento de los hechos, con una duración máxima inicial de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses». En todo caso, «la duración de la interceptación se computará desde la fecha de la autorización judicial» (Véase, apartado 16 del Manual de Orientaciones para la Práctica de Diligencias por la Policía Judicial). Muchos consideran que los plazos estipulados en ocasiones son demasiado lesivos para los derechos fundamentales, pues los dispositivos interceptados lo pueden estar hasta 18 meses.

Por otra parte, la Policía Nacional también se vale del Sistema de Integrado de Interceptación Telefónica (S.I.T.E.L.) para interceptar comunicaciones; tanto es así que cobró especial relevancia en la resolución de los Atentados del 11-M. Y lo hace en las mismas condiciones que se estipulan para la Policía Judicial de la Guardia Civil. En este sentido, la Policía Nacional, una vez obtenida la autorización judicial necesaria, contacta con el operador telefónico con el objetivo de que este le permita

monitorizar el terminal para posteriormente acceder a los contenidos y metadatos de las comunicaciones. Entre otros contenidos, se encuentran a qué hora se hizo uso del sistema, durante cuánto tiempo y en qué terminal. Después, toda esa información se almacenará en un disco duro con el fin de ser analizada por un experto en las Nuevas Tecnologías.

Junto con los anteriores requisitos, la prueba pericial informática tendrá por objeto el análisis de los dispositivos de almacenamiento de datos (en nuestro caso, el teléfono móvil), y en concreto tendrá que determinar el estado de las conversaciones que fueron aportadas en el proceso, esto es, tendrá que delimitar si los mensajes aportados fueron alterados, borrados o destruidos. Del mismo modo, es conveniente establecer el modelo del terminal, y la confirmación de envío y recepción de los mensajes. También, el artículo 478 de la L.E.Crim. establece que «el informe pericial comprenderá, si fuere posible: 1.º Descripción de la persona o cosa que sea objeto del mismo, en el estado o del modo en que se halle. El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes. 2.º Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior. 3.º Las conclusiones que en vista de tales datos formulen los peritos, conforme a los principios y reglas de su ciencia o arte».

Además, se ha discutido por la Jurisprudencia la necesidad de intervención de dos peritos informáticos con el objetivo de autenticar el sentido de las conversaciones aportadas en un proceso judicial concreto. Y es que el artículo 459 de la L.E.Crim. establece que «todo reconocimiento pericial se hará por dos peritos». Pues bien, los Tribunales de Justicia españoles son conscientes de la tardanza en aplicar Justicia y del encarecimiento del acceso a la misma, por lo que han entendido en los últimos años que la actuación de un solo perito no afecta en nada a la validez de la prueba, ni tampoco vulnera la tutela judicial efectiva prevista en el artículo 24 de la Constitución (véase, en este sentido, Sentencia de la Audiencia Provincial de Madrid de 8 de noviembre de 2011). En todo caso, habrá que atender a la complejidad del delito por el cual se acusa al investigado.

A todo esto hay que hacer una salvedad, y es que, para el procedimiento penal abreviado, el artículo 788.1 de la L.E.Crim. «contempla expresamente que en la fase de investigación propiamente dicha, conocida como diligencias previas, el informe pericial pueda ser prestado por un solo perito cuando el Juez lo considere suficiente»[76]. Esta tesis ha sido seguida por las Sentencias número 240/2013 del Tribunal Supremo, de 30 de enero, y número 1443/2013, de 18 de febrero. En la primera, se concluye que «la doctrina de esta Sala ha establecido en reiteradas ocasiones la plena validez del informe evacuado por un solo perito, dentro del procedimiento ordinario. […] Las previsiones de este precepto, que se entienden mejor si se tiene en cuenta la fecha en que fue redactado, demuestran que la dualidad

[76] http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUNjC1NDtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAuVjAuzUAAAA=WKE

de peritos se justifica en la búsqueda de una mayor certeza y rigor técnico, pero no es condición inexcusable del informe pericial que puede ser válido, en algunos casos, aun prestado por un solo perito» (F.J. 1º apartado 4º). Por el contrario en la segunda, se afirma que «la exigencia de dualidad de perito en cada dictamen pericial obedece a la mayor garantía de acierto que representa la posible coincidencia de pareceres de dos peritos frente a la opinión única […]. En tales casos, el mero dato formal de estar suscrito el informe por uno solo de los profesionales del equipo (...) no puede ocultar el hecho real de que el dictamen no es obra de un solo individuo, es decir, de un perito, sino del trabajo de equipo normalmente ejecutado según procedimientos científicos protocolizados en los que intervienen varios expertos, desarrollando cada uno lo que le compete en el común quehacer materializado por todos» (F.J. 6º).

Finalmente y tras lo dispuesto con anterioridad, podemos concluir que la única forma que hoy en día atribuye la eficacia jurídica necesaria para demostrar la autoría real y dar integridad a lo aportado es a través de la práctica de una prueba pericial informática. Así, el Legislador tiene que ser consciente de que la prueba electrónica presenta particularidades que la hacen muy distinta al resto de medios probatorios, de ahí que sea necesario recoger en nuestra Legislación, entre otros, los requisitos *sine qua non* para declarar una prueba pericial informática apta. En conclusión, se necesitan los siguientes requisitos para la aceptación de la prueba pericial informática[77]:

a) Que se respeten las exigencias de los artículos 340 y siguientes de la L.E.C.: se necesita que el perito tenga los conocimientos suficientes como para emitir el informe correspondiente.

b) Que se analice el soporte original de almacenamiento de la información, tanto desde el que se envió esta como el que la recibió.

c) Que se preserve y garantice la cadena de custodia, así como la aplicación de los protocolos de las Fuerzas y Cuerpos de Seguridad del Estado.

d) Que se analice el estado de las conversaciones que fueron aportadas en el proceso, esto es, que determine si los mensajes aportados fueron alterados, borrados o destruidos.

e) Que se respete el contenido del artículo 478 de la L.E.Crim.: o sea, que se describa el estado del terminal, que se haga una relación detallada de las operaciones practicadas por los peritos, y que se relaten las conclusiones del análisis practicado.

Se hace, por tanto, necesario desarrollar una Legislación que sea lo suficientemente sólida como para acabar con estas problemáticas, sobre todo cuando se ha demostrado por diversos peritos informáticos, entre otros por RUBIO ALAMILLO[78], que es

[77] Fuente: Elaboración propia.

[78] http://peritoinformaticocolegiado.es/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/

posible manipular un mensaje de *WhatsApp* siendo extremadamente complicado certificar pericialmente que fue efectivamente alterado. Es ineludible legislar para avanzar hacia una mayor seguridad jurídica.

3. *Protocolos para la autenticación: especial referencia a la norma ISO/IEC 27037:2012*

Anteriormente se ha desarrollado la cuestión de la aplicación de los distintos protocolos que resultan obligatorios para el proceder de las Fuerzas y Cuerpos de Seguridad del Estado. En cambio, hay que hacer un matiz, y es que se trata de protocolos que se centran en cómo obtener la prueba electrónica, en concreto en cómo interceptar lícitamente las comunicaciones del investigado para posteriormente ser analizadas. Ahora, por el contrario, se trata de estudiar aquellos protocolos que van dirigidos, no a la obtención de la prueba electrónica, sino a su autenticación. Fruto de la práctica forense, se han desarrollado en los últimos años guías o protocolos que tienen por objeto establecer el correcto proceso de identificación de los múltiples dispositivos electrónicos (entre otros, los de almacenamiento digital, los dispositivos móviles, los dispositivos conectados en red, las cámaras de vídeo o los sistemas móviles de navegación) para su posterior recolección, adquisición y preservación.

Entre estos, destaca por su habitual aplicación, en el ámbito informático, la Norma ISO/IEC 27037:2012: «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence». Y es que esta norma, adscrita al ámbito de la seguridad informática, desarrolla la «Guía para la identificación, recolección, adquisición y preservación de las evidencias digitales», y se ha constituido como el primer estándar a nivel mundial utilizado por los profesionales informáticos.

Así las cosas, ha resultado necesario «realizar una metodología aceptable para asegurar la integridad y autenticidad de la potencial evidencia digital»[79], pero no limitando nunca el manejo de métodos o herramientas para llevarlo a cabo. Su objetivo, entonces, es uniformar las actuaciones de los profesionales de las Nuevas Tecnologías, distinguiendo entre «Primeros Respondedores de Evidencia Digital» (o «Digital Evidence First Responders» –DEFRs–) y «Especialistas en Evidencia Digital» (o «Digital Evidence Specialist» –DESs–). Los primeros tendrán capacidad para recoger y adquirir la evidencia digital, mientras que los segundos tendrán la capacidad añadida de analizar la misma. De esta forma, los distintos especialistas actuarán en las fases sucesivas de identificación (entendida como la «localización e identificación de las potenciales evidencias de pruebas»), de recolección y adquisición (entendida como la «incautación y copia de los dispositivos y documentación que puedan contener la evidencia que se desea recopilar») y,

[79] http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012

finalmente, de conservación (ya que «las evidencias deben ser preservadas para poder ser útiles de cara a ser admitidas como pruebas»[80]).

A lo largo de esas etapas, se tendrá en cuenta que la evidencia digital ha de ser obtenida del modo menos intrusivo posible ya que debe preservarse la originalidad de la prueba y obtenerse copias de respaldo (es lo que se denomina por la norma como «Aplicación de Métodos»). También, la información obtenida debe haber sido contrastada por las buenas prácticas profesionales (lo que se denomina «Proceso Auditable») y debe de ser reproducible, verificable y argumentable al nivel de comprensión de los entendidos en la materia (denominado «Proceso Reproducible»). Y, finalmente, las herramientas utilizadas deben de ser mencionadas, teniendo que ser contrastadas en su uso para el fin en el cual se utilizan en la actuación («Proceso Defendible»).

En todo caso, la norma ISO no se queda ahí, sino que establece una serie de requerimientos para que la evidencia digital sea analizada conforme a la Legislación aplicable en cada momento y lugar. En otras palabras, «la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia»[81]. Así, la norma entiende por «relevancia» aquella «condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos».

En segundo lugar, por «confiabilidad» entiende aquella condición orientada a conocer si «la evidencia que se extrae u obtiene es lo que deber ser». Finalmente, por «suficiencia» entiende aquella condición por la cual «con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada».

Pues bien, de no ser respetados estos requerimientos, la autenticación de la evidencia electrónica no sería relevante, y estaría sometida a contradicción en el proceso judicial. En cualquier caso, «este estándar internacional no aborda la metodología para procedimientos legales, procedimientos disciplinarios, y otras acciones relacionadas al manejo de potencial evidencia digital, la cual está fuera del alcance de la identificación, recolección, adquisición y preservación»[82]. En otras palabras, a pesar de construirse como estándar internacional en el ámbito de la informática, poca ha sido la importancia que en el mundo jurídico se le ha dado.

En conclusión, es necesario avanzar en la creación de directrices que permitan identificar, recoger y preservar las evidencias electrónicas, pues ante todo debe de garantizarse la originalidad e integridad de aquello que se aporta en juicio. Y, sobre todo, es vital que nuestro Legislador proporcione los medios necesarios para que los

[80] http://wh0s.org/2014/06/21/estandares-de-manipulacion-de-pruebas-digitales-isoiec-270372012/

[81] http://insecurityit.blogspot.com.es/2013/09/reflexiones-sobre-la-norma-isoiec.html

[82] http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012

peritos informáticos puedan actuar con la cautela debida en la verificación de las pruebas electrónicas aportadas en el proceso penal, pues es frecuente que los dispositivos móviles queden involucrados en las investigaciones judiciales, o sea, normalmente lo primero que se investiga al cometerse un hecho delictivo es que se haya llevado a cabo en presencia de un teléfono móvil. Se trata, pues, no sólo de confiar en mecanismos de autenticación como el expuesto, sino que se dé cumplimiento veraz a lo recogido por nuestra Legislación en materia de derechos fundamentales. Hay que ser conscientes de que, dada la fragilidad de las pruebas electrónicas, es necesario realizar una metodología aceptable para asegurar la integridad y autenticidad de la prueba electrónica; aún más cuando la forma de comunicarnos ha cambiado y no se sabe la magnitud de los avances que la Tecnología pueda llevar a cabo en los próximos años. Se trata de que a más autenticación, mayor seguridad jurídica.

VI. CONCLUSIONES: HACIA UNA *JUSTICIA 2.0*

Llegado este punto, hay dos ideas básicas que es necesario traer a colación. La primera va dirigida a entender que, a pesar de que la prueba electrónica viene a admitirse y valorarse positivamente por la Justicia, lo cierto es que sufre de numerosas debilidades; y no solo eso sino que, de no ser mitigadas, se agravarán con el paso del tiempo. Por el contrario, la segunda idea va encaminada a cuestionar el trabajo del Legislador, ya que contamos con una Legislación defectuosa e incompleta (desgraciadamente algo habitual en el proceso penal). Así las cosas y teniendo en cuenta estas dos ideas–faro, se formulan las siguientes propuestas:

PRIMERA. En relación con la definición de prueba electrónica y dado que ha resultado ser la *rara avis* de entre todos los medios de prueba que se enumeran en el artículo 299 de la L.E.C., es ineludible que el Legislador precise de forma inmediata lo que entiende por prueba electrónica. En este sentido, es necesario establecer legislativamente los elementos que configuran este medio probatorio, por ejemplo con la implantación de un sistema que permita una clara diferenciación respecto de los medios de reproducción de la palabra, el sonido y la imagen, así como aquellos otros que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase. Por ello, es necesario otorgar mayor seguridad jurídica a nuestro Ordenamiento jurídico, sobretodo dado el uso cada vez mayor de los nuevos medios de comunicación, entre los cuales se sitúa *WhatsApp*.

Así las cosas, un concepto que encajaría perfectamente con lo que hemos entendido a lo largo de este Trabajo por prueba electrónica sería el dado por DELGADO MARTÍN, pues la definía como «toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio», refiriéndose «a cualquier clase de información; que ha ser producida, almacenada o transmitida por medios electrónicos; y que pueda tener efectos para acreditar hechos en el proceso abierto para la investigación de todo tipo de infracciones penales, y no solamente

para los denominados delitos informáticos»[83]. Del mismo modo, se podría tener en consideración la definición dada por BUENO DE MATA cuando la reduce a «cualquier información obtenida a partir de un dispositivo electrónico o medio digital que sirva para adquirir convencimiento de la certeza de un hecho, siempre que sea correctamente obtenida, constituyendo así pruebas exactas, veraces y objetivas», esto es, se trata de «aquel medio electrónico que permite acreditar hechos relevantes para el proceso, ya sean físicos o incluso electrónicos, y que se compone de dos elementos necesarios para su existencia, los cuales delimitan la especialidad de la prueba electrónica en relación al resto de medios probatorios: un elemento técnico o *hardware*, y un elemento lógico o *software*»[84].

SEGUNDA. Al igual que se necesita configurar un concepto legal de prueba electrónica, es inevitable considerarla como un medio de prueba autónomo e independiente de lo que son otros medios probatorios. Esto es, la prueba electrónica en sí misma no puede ser enmarcada dentro del artículo 299.2 de la L.E.C., pues no se trata de un medio de reproducción de la palabra, el sonido y la imagen ni de un instrumento que permite archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas, sino que se trata de un medio al cual se le aplica la cláusula abierta recogida en el apartado tercero del artículo 299.

Por lo tanto, resultar obligatorio reformar el contenido del artículo 299 de la L.E.C., estableciendo una nueva regulación del artículo 299 de la L.E.C., alejada del *numerus clausus* del artículo 299.1 de la L.E.C. Para ello, se puede tener en consideración la propuesta de regulación dada por BUENO DE MATA, quedando el apartado segundo de este precepto de la siguiente manera:

> «También se admitirá cualquier fuente de prueba que pudiera ser originada por el desarrollo tecnológico, científico o informático, la cual será incorporada a través de los medios probatorios regulados en el apartado anterior, siempre que de ellas pudiera obtenerse certeza sobre hechos relevantes. El tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias para su correcta incorporación al proceso

De esta forma, la regulación conseguiría mitigar el avance de la Sociedad y la aparición de nuevos acontecimientos sociales, económicos, tecnológicos, etc. que pudieran desarrollarse durante los próximos años.

TERCERA. También, resulta necesario regular de forma específica, real y completa la prueba electrónica, sobre todo en lo que tiene que ver con su obtención, aportación y posterior valoración. En este sentido, el Legislador tiene que prever normativamente la colisión que se produce a la hora de obtener la prueba electrónica

[83] DELGADO MARTÍN, J.: «La prueba… *op.*, cit, pág. 1.

[84] BUENO DE MATA, F.: *Prueba electrónica… op.*, cit, pág. 103.

con respecto de los derechos fundamentales cuya titularidad ostenta el investigado. Y es que, es inexcusable que prevea la ponderación entre los bienes jurídicos que han resultado dañados por la comisión de un hecho delictivo y derechos tan importantes como el derecho a la intimidad personal, a la autodeterminación informativa, al secreto de las comunicaciones, a la inviolabilidad domiciliaria, a la protección de datos de carácter personal y al deber de preservación de la cadena de custodia.

Del mismo modo, no pueden aplicarse automáticamente, entre otros, los artículos 382 a 384 de la L.E.C., pues están previstos para los instrumentos de filmación y grabación que recoge el apartado segundo del artículo 299. Se trata, entonces, de abandonar la aplicación analógica de una normativa repleta de lagunas y que otorga más bien poca seguridad jurídica, y desarrollar otra en la que se prevean las especialidades de la prueba electrónica, así como su complejidad técnica y vulnerabilidad. Ha de ser una regulación que, además, evite la dispersión normativa con la que hoy en día contamos.

CUARTA. Por otra parte, es necesario fomentar judicialmente el uso de medidas de aseguramiento de la prueba electrónica, pues otras de carácter tradicional, como el depósito, resultan insuficientes. En este sentido, la institución del aseguramiento de la prueba cobra especial relevancia a la hora de hablar de la prueba electrónica, ya que el riesgo de manipulación, borrado o destrucción del contenido de *WhatsApp* hace preciso que se prevean y desarrollen legislativamente figuras como el *hash*, el Sistema de Sellado de Tiempo «TSA - Time Stamp Authority» u otras formas de certificación y custodia de las pruebas electrónicas. Por consiguiente, el contenido de los artículos 297 y 298 de la L.E.C. es insuficiente dada la complejidad de estas aplicaciones de mensajería instantánea.

QUINTA. De la misma forma, sería conveniente fomentar el uso de ciertas técnicas de aportación de la prueba electrónica al proceso penal (como la prueba pericial informática), y abandonar otros métodos que ofrecen escasa eficacia jurídica (como serían los «pantallazos»). Pues bien, al igual que el Legislador ha innovado y ha avanzado hacia la adaptación de la Justicia a las Nuevas Tecnologías (por ejemplo, con la implantación del sistema LEXNET), resulta necesario regular los medios idóneos a la hora de aportar una conversación de *WhatsApp* al proceso penal. En este sentido, hay que tener claro que el rango de validez de los *WhatsApp* como prueba en un juicio va ligado a la técnica mediante la cual se hayan aportado al proceso, por lo que prácticas habituales como los «pantallazos» o la entrega de unidades de almacenamiento son poco eficaces a la hora de demostrar hechos controvertidos.

SEXTA. Respecto de la valoración de la prueba electrónica en el proceso penal, lo que está claro es los Tribunales de Justicia españoles aplican la regla general consistente en el otorgamiento de valor probatorio a las conversaciones de *WhatsApp*. Sin embargo, resulta indispensable regular legislativamente la validez de estas conversaciones, pues la prueba electrónica habrá de practicarse con todas las garantías en la vista oral, respetándose los principios de contradicción, oralidad e inmediación. Es conveniente, así, el establecimiento de unos criterios de validez de las distintas técnicas que pueden ser utilizadas para incorporar las conversaciones de *WhatsApp* al proceso penal. Y, a esto hay que añadir, que la doctrina jurisprudencial resulta confusa e insuficiente, hasta tal punto de que se corre el riesgo de privatizar el proceso penal, condicionando la posibilidad de condena a la capacidad económica de la víctima en función de si es posible que aporte, o no, un informe pericial informático de parte para apoyar la autenticidad de los *WhatsApp* aportados. Sería, entonces, conveniente que el Tribunal sea el que de oficio solicite la actuación de un perito informático.

SÉPTIMA. También, es necesario que el Legislador prevea la práctica de las diligencias de investigación y tenga en cuenta las incidencias que se dan respecto de las políticas de privacidad que resultan exigibles por los proveedores de los servicios de mensajería instantánea. Esto es, resulta conveniente que se endurezca la exigencia del deber de colaboración que se recoge en el artículo 588 *septies* b de la L.E.Crim., pues muchas veces las empresas no permiten que las investigaciones se desarrollen con la rapidez y eficacia necesarias, de manera que torpedean la investigación de un hecho delictivo. En este sentido, hay que tener en cuenta que la activación del cifrado «E2EE» por parte de la compañía *WhatsApp* puede contravenir de manera amplia ese deber de colaboración que se recoge en nuestra Legislación respecto de los prestadores de servicios enumerados en el artículo 588 *ter* e de la L.E.Crim.

OCTAVA. Por otro lado y con respecto a las diligencias de investigación, resulta requisito *sine qua non* la aplicación estricta de los protocolos existentes para el proceder de las Fuerzas y Cuerpos de Seguridad del Estado. En este sentido, es conveniente que las Fuerzas y Cuerpos de Seguridad del Estado sean conscientes de que deben cumplirse las exigencias inherentes a nuestro Estado de Derecho, pues existe una línea estrecha entre la obtención lícita de una prueba electrónica y la intervención ilegítima de los dispositivos móviles. Ante todo, las garantías constitucionales básicas deben ser respetadas, garantizándose, entre otras, la tutela judicial efectiva y el desarrollo de un debido proceso, con las características de justo, pronto y transparente.

NOVENA. También, en materia de autenticación de la prueba electrónica, resulta indispensable fomentar y regular los protocolos para la autenticación de la prueba electrónica. Esto es, normas, como la ISO/IEC 27037:2012: «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», pueden acabar de forma objetiva con el problema de la autoría y manipulación de las conversaciones de *WhatsApp*. De esta forma, la práctica de prueba pericial informática (siguiendo los protocolos de autenticación que se prevean en su momento) es la única forma que hoy en día existe para demostrar de manera objetiva y puntual que un mensaje de *WhatsApp* es original, o efectivamente fue manipulado, borrado o destruido.

DÉCIMA. Por todo ello, el Legislador tiene que ser consciente de que el Derecho debe ser adaptado a los nuevos acontecimientos sociales, económicos y tecnológicos, aún más cuando nuestra Justicia no está preparada para mitigar los efectos que los nuevos medios de comunicación provocan con el paso del tiempo. Resulta, por tanto, necesario modificar tanto la L.E.C. como la L.E.Crim. en materia de prueba electrónica, ya que la Tecnología evoluciona a un ritmo completamente distinto a como lo hace el sistema judicial. Del mismo modo, de nada sirve que la regulación estatal sea adaptada a los nuevos tiempos, ya que, de haber una regulación dispar en cada país de la Unión Europea, nada se solventaría dado el nivel de globalización en el que hoy en día vivimos. Por eso, el Legislador comunitario tiene que establecer las bases necesarias para avanzar hacia una *Justicia 2.0*, para después ser desarrolladas y aprovechadas por el Legislador estatal.

V. RESEÑA BIBLIOGRÁFICA

▪ Bibliografía principal

- ALONSO-CUEVILLAS SAYROL, J.: «Internet y prueba civil», *Revista Jurídica de Cataluña*, Vol. 100, núm. 4, Barcelona, 2011.
- BACARIA MARTRUS, J.: «El caso WhatsApp. Las aplicaciones de mensajería instantánea como medio de prueba en el procedimiento judicial», *Economist & Jurist*, Vol. 22, nº 185, noviembre 2014.
- BUENO DE MATA, F.: *Prueba electrónica y proceso 2.0. Especial referencia al proceso civil*, Ed. Tirant lo Blanch, Valencia, 2014.
- CARNELUTTI, F.: *La prueba civil*, 2ª edición, Ed. Ediciones Depalma, Buenos Aires, 2000.
- DE URBANO CASTILLO, E.: *La valoración de la prueba electrónica*, Ed. Tirant lo Blanch, Valencia, 2009.
- DELGADO MARTÍN, J.: «La prueba del WhatsApp», *Diario La Ley*, nº 8605, Sección Tribuna, Ed. LA LEY, 2015.

- DELGADO MARTÍN, J.: «La prueba electrónica en el proceso penal», *Diario La Ley*, nº 8167, Sección Doctrina, Ed. LA LEY, 2013.
- GINÉS CASTELLEY. N. (Coord.) y otros: «Prueba electrónica», *La prueba electrónica,* Colección de Formación continua Facultad Derecho ESADE, Serie Estudios Prácticos sobre los medios de prueba, nº 5, Barcelona, 2011.
- GÓMEZ DEL CASTILLO Y GÓMEZ, M.: «Aproximación a los nuevos medios de prueba en el proceso civil», *Revista Derecho y conocimiento de la Facultad de Derecho de la Universidad de Huelva*, Vol. I, 2001.
- ILLAN FERNÁNDEZ, J.M.: *La prueba electrónica, eficacia y valoración en el proceso civil,* Ed. Aranzadi, Navarra, 2009.
- ILLÁN FERNÁNDEZ, J.M.: *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil. Nueva Oficina Judicial, Comunicaciones Telemáticas (LEXNET) y el Expediente Judicial Electrónico. Análisis Comparado Legislativo y Jurisprudencial*, Navarra, 2009.
- JURADO SALAZAR, A.: «Valor probatorio del documento electrónico», *Cuestiones Jurídicas, Revista de Ciencias Jurídicas de la Universidad Rafael Urdaneta*, Vol. V, nº 1 (Enero-Junio 2011), Maracaibo, Venezuela, 2011.
- OLIVA LEÓN, R. (Coord.) y otros: «La prueba electrónica envenenada», *La prueba electrónica: validez y eficacia procesa*l, Colección Desafíos Legales #RetoJCF, Juristas con Futuro, 2016.
- PEREIRA PUIGVER, S.: «Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte», *Fodertics II: Hacia una justicia 2.0. Estudios Sobre Derechos y Nuevas Tecnologías*, Ed. Ratio Legis, Salamanca, 2014.
- PEREIRA PUIGVERT, S.: *La Exhibición de Documentos Probatorios y Soportes Informáticos*, Ed. Aranzadi, Navarra, 2013.
- PÉREZ PALACI, J.E.: *La prueba electrónica: Consideraciones,* 2014 [Recurso electrónico: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39084/1/PruebaElectronica2014.pdf].
- SÁNCHEZ HERNÁNDEZ, J.: «¿WhatsApp, prueba válida en juicio?»**,** *PorDerecho.com*, nº. 12 – 2016, Revista del Ilustre Colegio de Abogados de Salamanca, Salamanca, 2016.
- SENTIS MELENDO, S.: *La prueba. Los grandes temas del derecho probatorio*, Ed. Ediciones Jurídicas Europa-América, Vol. 65, Buenos Aires, 1979.
- SOTO CALDERA, M.M.: «Consideraciones sobre la prueba documental electrónica en el proceso civil venezolano», *Estudios de derecho civil,* Vol. III, Libro homenaje a José Luis Aguilar Gorrondona, Tribunal Supremo de Justicia, Colección Libros homenaje nº. 5, 2001.
- VILLACAMPA ESTIARTE, C.: *Stalking y Derecho Penal. Relevancia Jurídico-Penal de una Nueva Forma de Acoso*, Ed. Iustel, Madrid, 2009.

▪ Prensa digital

- «El 40% de los 'whatsApps' y SMS usados en juicios son falsos, según la Asociación de Internautas», *Diario Público*, 22 de agosto de 2014.
- «España, el cuarto país en el mundo en el uso de WhatsApp», Diario *ABC*, 25 de febrero de 2015.
- «Las «aplastantes» cifras de WhatsApp: 2.000 millones de mensajes al día, 1.600 millones de fotos y 250 millones de vídeos», Diario *ABC*, 2 de febrero de 2016.
- «Las contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo», Sección Conocimiento, Artículos Doctrinales, *Noticias Jurídicas*, 30 de septiembre de 2015.
- «WhatsApp hace historia: supera los 1.000 millones de usuarios activos al mes», Diario *elEconomista.es*, 2 de febrero de 2016.

▪ Sitios Web

- http://ala.org.es/la-validez-probatoria-del-whatsapp-y-su-incorporacion-al-procedimiento/
- http://ceaj.es/i-premio-monografico-2016-nulidad-de-la-prueba-por-vulneracion-del-art-18-4-ce-por-carlos-donoro-ayuso/
- http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNjC1NDtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAuVjAuzUAAAA=WKE
- http://insecurityit.blogspot.com.es/2013/09/reflexiones-sobre-la-norma-isoiec.html
- http://peritoinformaticocolegiado.es/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/
- http://web.icam.es/bucket/ponencia-prueba-electronica.pdf
- http://wh0s.org/2014/06/21/estandares-de-manipulacion-de-pruebas-digitales-isoiec-270372012/
- http://www.audea.com/es/herramientas/certificacion-y-acta-de-prueba-electronica/
- http://www.elconfidencial.com/espana/2016-10-25/whatsapp-diana-quer-guardia-civil_1279664/
- http://www.genbeta.com/movil/whatsapp-envia-sus-mensajes-encriptados-pero-su-seguridad-sigue-siendo-baja
- http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal
- http://www.mjusticia.gob.es/cs/Satellite/Portal/1292387342364?blobheader=application%2Fpdf&blobheadername1=Content-

Disposition&blobheadervalue1=attachment%3B+filename%3DPropuesta_texto_articulado_L.E.Crim..PDF

- http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-troyano/
- http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7100605&links=&optimize=20140619&publicinterface=true
- http://www.poderjudicial.es/stfls/SALA%20DE%20PRENSA/NOTAS%20DE%20PRENSA/TSPenal%2027.11.15%20(10333-15).pdf
- http://www.redeszone.net/2015/10/02/asi-se-pueden-falsificar-los-mensajes-de-whatsapp/
- http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012
- https://blog.kaspersky.com.mx/que-es-un-hash-y-como-funciona/2806/
- https://doyfe.es/
- https://hipertextual.com/archivo/2014/01/acceso-root-android/
- https://securityinabox.org/es/tor_principal
- https://ws024.juntadeandalucia.es/ae/adminelec/areatecnica/notario
- https://www.avast.com/es-es/c-malware
- https://www.infospyware.com/articulos/que-son-los-spywares/

▪ Legislación

- Constitución Española de 1978.
- Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950.
- Decreto de 2 junio 1944, *por el que se aprueba con carácter definitivo el Reglamento de la organización y régimen del Notariado.*
- Ley 1/2000, de 7 de enero, *de Enjuiciamiento Civil.*
- Ley 11/2007, de 22 de junio, *de acceso electrónico de los ciudadanos a los Servicios Públicos.*
- Ley 18/2011, de 5 de julio, *reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.*
- Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*
- Ley 34/2002, de 11 de julio, de *Sociedad de Servicios de la Información y de Comercio Electrónico.*
- Ley 42/2015, de 5 de octubre, *de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil*.
- Ley 59/2003, de 19 de diciembre, *de firma electrónica.*
- Ley 9/2014, de 9 de mayo, *General de Telecomunicaciones.*

- Ley Orgánica 1/1982, de 5 de mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
- Ley Orgánica 1/2015, de 30 de marzo, *por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*.
- Ley Orgánica 10/1995, de 23 de noviembre, *del Código Penal.*
- Ley Orgánica 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.*
- Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal.*
- Ley Orgánica 6/1985, de 1 de julio, *del Poder Judicial.*
- Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2011.
- Real Decreto 1065/2015, de 27 de noviembre, *sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET.*
- Real Decreto de 14 de septiembre de 1882, *aprobatorio de la Ley de Enjuiciamiento Criminal.*

▪ Jurisprudencia (ordenado por órganos jurisdiccionales)

o Tribunal Constitucional

- Sentencia del Tribunal Constitucional número 1/2004, de 14 de enero.
- Sentencia del Tribunal Constitucional de 29 de septiembre de 2003.
- Sentencia del Tribunal Constitucional número 236/2002, de 9 de diciembre.
- Sentencia del Tribunal Constitucional número 147/2002, de 15 de junio.
- Sentencia del Tribunal Constitucional número 70/2002, de 3 de abril.
- Sentencia del Tribunal Constitucional (Pleno) número 10/2002.
- Sentencia del Tribunal Constitucional número 173/2000, de 26 de junio.
- Sentencia del Tribunal Constitucional número 11/1984, de 29 de noviembre.
- Sentencia del Tribunal Constitucional número 22/1984, de 17 de febrero.
- Auto del Tribunal Constitucional número 569/1983, de 23 de noviembre.

o Tribunal Supremo

- Sentencia del Tribunal Supremo número 329/2016, de 20 de abril.
- Sentencia del Tribunal Supremo número 300/2015, de 19 de mayo.
- Sentencia del Tribunal Supremo número 587/2014.
- Sentencia del Tribunal Supremo número 1443/2013, de 18 de febrero.
- Auto del Tribunal Supremo de 14 de febrero de 2013.

- Sentencia del Tribunal Supremo número 240/2013, de 30 de enero.
- Sentencia del Tribunal Supremo número 785/2008, de 25 de noviembre.
- Sentencia del Tribunal Supremo número 511/1999, de 24 de marzo.

o Tribunales Superiores de Justicia

- Sentencia del Tribunal Superior de Justicia de Andalucía (Málaga), de 28 de enero de 2000.

o Audiencias Provinciales

- Sentencia de la Audiencia Provincial de Burgos número 189/2016, de 13 de mayo.
- Sentencia de la Audiencia Provincial (Sección 6ª) número 365/2015, de 11 de noviembre.
- Sentencia de la Audiencia Provincial de Zaragoza número 89/2015, de fecha 17 de septiembre.
- Sentencia de la Audiencia Provincial de Granada (Sección 1ª) número 486/2014, de 18 de septiembre.
- Sentencia de la Audiencia Provincial de Madrid número 533/2014, de 24 de julio.
- Sentencia de la Audiencia Provincial de Barcelona número 143/2014, de 7 de mayo.
- Sentencia de la Audiencia Provincial de Córdoba número 159/2014, de 2 de abril.
- Sentencia de la Audiencia Provincial de Cádiz número 31/2014, de 28 enero.
- Sentencia de la Audiencia Provincial de Pontevedra número 10/2014, de 10 enero.
- Sentencia de la Audiencia Provincial de Alicante número 4/2014, de 9 de enero.
- Sentencia de la Audiencia Provincial de Barcelona número 1396/2013, de 7 de noviembre.
- Sentencia de la Audiencia Provincial de Madrid número 51/2013, de 23 de septiembre.
- Sentencia de la Audiencia Provincial de Madrid número 12/2013, de 5 abril.
- Sentencia de la Audiencia Provincial de Madrid número 1260/2012, de 1 octubre.
- Auto de la Audiencia Provincial de Cantabria (Sección 3ª) número 291/2012, de 25 de mayo.
- Sentencia de la Audiencia Provincial de Madrid de 8 de noviembre de 2011.
- Sentencia de la Audiencia Provincial de Barcelona de 2 de mayo de 2007.

o Juzgados de lo Penal

- Sentencia del Juzgado de lo Penal de Teruel número 98/2016, de 16 de junio.

o Juzgados de Violencia Sobre la Mujer

- Sentencia del Juzgado de Violencia sobre la Mujer número 1 de Granada número 50/2016, de 20 de junio.

- Juzgados de Primera Instancia e Instrucción

  - Sentencia del Juzgado de Primera Instancia e Instrucción número 1 de Moncada (Valencia) de 30 de diciembre de 2015.
  - Auto del Juzgado de Primera Instancia e Instrucción nº 1, de fecha 15 de marzo de 2013.
  - Sentencia del Juzgado de Primera Instancia de Murcia número 69/2007, de 30 de marzo.

- Otros

  - Guía S.O.S. contra el Grooming. Padres y educadores, Instituto Nacional de Tecnologías de la Comunicación INTECO), Ministerio de Industria, Energía y Turismo.
  - Acuerdo de 28 de octubre de 2010, del Pleno del Consejo General del Poder Judicial, *por el que se modifica la Instrucción 5/2001, de 19 de diciembre, del Consejo, sobre remisión anual a los órganos jurisdiccionales de las listas profesionales para su designación judicial como peritos y del Protocolo de actuación del servicio común procesal para la asignación de peritos judiciales, de 9 de febrero de 2005*.
  - Circular de la Fiscalía General del Estado número 1/2013, *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*.
  - Instrucción número 5/2001, de 19 de diciembre de 2001, del Pleno del Consejo General del Poder Judicial *sobre remisión anual a los órganos jurisdiccionales de listas de profesionales para su designación judicial como peritos.*
  - Manual de Orientaciones para la Práctica de Diligencias por la Policía Judicial de 24 de febrero de 2016.
  - Manual del Servicio de Policía Judicial de la Guardia Civil de 31 de mayo de 2011.
  - Norma ISO/IEC 27037:2012: «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.
  - Propuesta de Texto Articulado de Ley de Enjuiciamiento Criminal, por la Comisión Institucional creada por Acuerdo de Consejo de Ministros de 2 de marzo de 2012.
  - Resolución número 56/121 aprobada por la Asamblea General de la Organización de las Naciones.
  - Resolución número 55/63 aprobada por la Asamblea General de la Organización de las Naciones.