IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Dosier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»

ARTÍCULO

Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre*

Teresa Armenta Deu
Universitat de Girona

Fecha de presentación: mayo de 2018
Fecha de aceptación: julio de 2018
Fecha de publicación: septiembre de 2018

Resumen

Este estudio se centra en los medios tecnológicos como fuente de investigación en el proceso penal y, más concretamente, en tres fuentes de prueba digital: los correos electrónicos, los WhatsApp, y las redes sociales. Con el objetivo central de analizar la valoración probatoria y las especificidades de aquellos, se ha querido partir de la insuficiente regulación legal hasta la reforma de 2015 y el cuestionamiento actual de la idoneidad de esta última. Entre ambas, el examen pormenorizado de la doctrina y jurisprudencia sobre las fuentes de prueba digital, que nos llevan a apreciar la necesidad de acomodar la legislación a las garantías constitucionales y europeas, afrontando paralelamente las dificultades que comportan unas técnicas digitales en constante evolución a la hora de adecuarse a las garantías probatorias.

Palabras clave

investigación tecnológica, valor probatorio, nulidad, fuentes de prueba digital

Tema

prueba tecnológica y proceso penal

* Este trabajo ha sido realizado disfrutando del I+D (referencia DER2017-82146-P) y de la Ayuda para la mejora de la productividad científica de los grupos de investigación (MPC UdG 2016/002).

Legal regulation and weighing up digital evidence (emails, WhatsApp, social networks): caught between insufficiency and uncertainty

Abstract

This study focuses on technological media as a source of criminal procedural research, looking at three sources of digital evidence in particular: emails, WhatsApp and social networks. With the primary aim of analysing how the evidence is weighed up and the specific features of this technological media, the study is based on the insufficient legal regulation until the reform of 2015, and the current doubts as to whether or not the latter is suitable. The detailed exam of the doctrine and the precedent set for the sources of digital evidence lead us to consider the need to adjust the legislation to constitutional and European guarantees, simultaneously dealing with the difficulties of some constantly evolving digital techniques when it comes to complying with evidentiary guarantees.

Keywords

technological investigation, evidentiary value, nullity, digital evidence sources

Topic

technological evidence and criminal proceedings

INTRODUCCIÓN: Consideraciones generales

El desarrollo de las comunicaciones ha generado una tremenda dependencia en el usuario que vierte una cantidad ingente de datos a través de internet en redes sociales, WhatsApp y otras aplicaciones de mensajería instantánea. Lo cierto es que la vida actual ofrece un número muy significativo de casos en que la tecnología es el medio utilizado para delinquir o la fuente básica para el desarrollo de la investigación.[1] Esta doble perspectiva abarca un sinfín de aspectos imposibles de abordar ahora: desde el amplio espectro de la «nueva criminalidad» que ofrecen estos medios,[2] hasta la utilización de recursos tecnológicos que van aumentando conforme se escriben estas líneas.[3] Todos inciden en un campo sujeto a un difícil equilibrio: la mayor eficacia en la represión de los delitos, en general, pero también en ámbitos como el terrorismo, la criminalidad organizada o los delitos que implican a menores de edad; y paralelamente, el respeto y protección no solo de los derechos fundamentales, mediante instrumentos como la prueba ilícita, sino también en el conjunto de las garantías procesales incorporadas en el derecho a la presunción de inocencia y el derecho al debido proceso.[4]

Centrándonos en los medios tecnológicos como fuente esencial de muchas investigaciones, la ingente bibliografía sobre la prueba en la era digital, de internet como fuente

1. Las nuevas tecnologías en el enjuiciamiento penal ofrecen un doble enfoque: como objeto y como instrumento (Delgado Martín, 2016, capítulo, I, nota 5).
2. Asencio Mellado y Fernández López (2017).
3. Cabezudo Rodríguez (2016, pág. 9).
4. Desde el 11-S, el atentado en Londres y el 5-M, se incrementaron los instrumentos investigadores y represores, que los más recientes atentados yihadistas (París, Berlín, Niza, Barcelona) no han hecho sino afianzar, generando el consiguiente movimiento pendular entre la doble necesidad de que el Estado persiga los delitos y simultáneamente la protección de los derechos inherentes a la dignidad de las personas, cuya realización y preservación es el fundamento de la legitimación del poder y de la validez del derecho que crea (Armenta Deu, 2014, pág. 229-252; Delgado Martín, *op. cit.*, cap. II).

de prueba o de la prueba tecnológica,[5] eximen de analizar algunos aspectos, pero no de situar al lector en la realidad pasada y presente que se inicia mediante un brevísimo repaso de la situación normativa que ha corrido paralela a esta vorágine tecnológica.

2. La situación hasta 2015: carencias normativas e interpretación jurisprudencial

Hasta fechas relativamente recientes, la detención de la correspondencia privada, postal telegráfica y telemática que el procesado remitiere o recibiere y su apertura y examen se regía, por analogía, por el artículo 579 LECrim. Con tales mimbres se afrontó la legalidad de múltiples medidas adoptadas para investigar asuntos, en un contexto social complejo,[6] conscientes de la insuficiencia normativa e intentando soslayar entre otros efectos indeseados las condenas de tribunales nacionales e internaciones.

En cuanto a la protección de datos generados por el tratamiento de los dispositivos de almacenamiento masivo, la obsoleta regulación interna contenida en el Reglamento de aspectos accesorios a las actuaciones jurisdiccionales 1/2005, de 16 de septiembre y el artículo 230.5 LOPJ, que aseguraba el cumplimiento de la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, fue objeto de revisión por la publicación de diversas directivas europeas hasta la Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; modificada posteriormente por la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Ambas anuladas por las STJUE, de 8 de abril de 2014 (asunto Digital Rights) y de 21 de diciembre de 2016 (asunto Tele2 Sverige), poniendo de relieve la precariedad de las exigencias legales requeridas para conservar datos de carácter personal.[7]

Como se ha adelantado, la jurisprudencia nacional e internacional fue reiterando la necesidad de cambios legislativos a través de importantes resoluciones de las que se citan algunas de las más destacadas.

La STS de 19 de julio de 2001 denunció una vez más la insuficiencia del artículo 579 LECrim para sustentar las investigaciones a través de medios tecnológicos, concretamente la ausencia de previsión de supuestos que justifican la intervención, el objeto y el procedimiento de ejecución de la medida, así como la trascripción en acta del contenido de los soportes magnéticos, la custodia y destrucción de las cintas.

Posteriormente, la STC de 23 de octubre 2003 incidió en la falta de regulación sobre el plazo máximo de la duración de las intervenciones, por no existir prórrogas; resaltando, además, un aspecto significativo: que el artículo 579 LECrim solo habilita para limitar el secreto de las comunicaciones de las personas sospechosas, pero no de terceros con quienes aquellos se comunican. Particularmente rotunda fue la STC 145/2014, de 22 de septiembre, recordando, no obstante, que dicha insuficiencia no significa que el derecho vulnerara el artículo 8 CEDH, sino que correspondía al TC suplir las insuficiencias apreciadas en el precepto legal citado (sic 579) hasta que se produzca la necesaria intervención del legislador; función integradora que, sin embargo, en casos como el resuelto no alcanza a supues-

5. A título indicativo: Bueno de Mata (2017); Magro Servet (2006, pág. 107-115); Castillejo Manzanares (2010, pág. 11-43); Urbano Castrillo (2011); Delgado Martín (2017); Portal Manrubia (2013, pág. 19-41); Garrido Carrillo (2013-2014, pág. 553-590); Pinto Palacios y Puyol Capilla (2017); Vervaele (2012, pág. 27-86); Encinar del Pozo y Villegas García (2017).
6. La realidad española de escalada terrorista de principios de los ochenta lleva al Ejecutivo a abordar la regulación de las «observaciones telefónicas», dictando la LO 9/84 de 26 diciembre, contra la actuación de bandas armadas y elementos terroristas. Y como reacción contra la posible arbitrariedad en las medidas de vigilancia secretas ordenadas por las facultades discrecionales concedidas, surgió la tipificación en los artículos 192 bis y 497 bis CP, relativos a la colocación ilegal de escuchas telefónicas, introducidos por la LO 7/84 EDL1984/9281. En el ámbito procesal penal, sin embargo, no se acometió la reforma del obsoleto artículo 579 LECrim hasta la LO 4/1988 de 25 mayo 1988. *Cfr*. Gallego Sánchez (2010). Sobre la prueba ilícita, en esta tesitura, Armenta Deu, (2014, *op. cit*., pág. 235-237).
7. Gudín Rodríguez-Magariños (2017).

tos no contemplados en la norma, como la intervención de una conversación verbal entre personas detenidas a través del móvil.[8]

El TEDDHH, por su parte, en sentencia de 18 de febrero de 2003 (caso Prado Burgallo c. España) volvió a incidir sobre la ya denunciada carencia.[9]

En lo relativo a la protección de datos, las citadas resoluciones del TEJUE (casos Digital Rights y Tele2 Sverige)[10] pusieron de relieve que la regulación europea sobrepasaba los límites que exige el respeto al principio de proporcionalidad requeridos por los artículos 7, 8 y 52.1 de la CEDH de la Unión Europea, lo que condujo a declarar invalidada la Directiva 2006/24/CE.[11] Esta anulación no ha dejado de suscitar serias dudas sobre el efecto sobre la legislación española mediante la trasposición de la citada Directiva 2006, *ex* Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. De hecho varios autores entienden que la STJUE de 21 de diciembre de 2016 sí ha afectado a la Ley 25/2007, derogándola de facto.[12] El pasado 10 de noviembre, el Gobierno aprobó el proyecto de una nueva Ley orgánica de protección de datos no así de la Ley de Enjuiciamiento Criminal.[13]

3. La reforma de 2015

La LO 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, acometió la reclamada regulación, enfocando rectamente las medidas de investigación tecnológicas en muy diversos supuestos y estableciendo incluso unos «principios rectores» que recogían la jurisprudencia recaída durante años en torno a los presupuestos que deben concurrir para toda medida limitativa de derecho fundamental.[14]

Los medios de investigación tecnológica se centran en dos fuentes: los procesos comunicativos y los dispositivos y sistemas informáticos de almacenamiento de datos. Sobre los primeros recaerán eventualmente diversas medidas: a) la intervención de las comunicaciones sostenida a través de tecnologías de la información, y una modalidad de interceptación de comunicaciones personales efectuadas a través de servicios, como el correo electrónico, WhatsApp y similares o por redes sociales en general, y b) la propia red pública que sustenta estas comunicaciones. En lo referente a los dispositivos y sistemas informáticos y

8. Tal era el caso resuelto en el que se otorgó el amparo solicitado por no respetarse que la medida de intervención fuera previsible para la persona afectada; no existiendo parámetros que marcaran el alcance de la discrecionalidad conferida a las autoridades competentes y la manera de su ejercicio, con la suficiente claridad como para proporcionar a las personas la protección adecuada contra una injerencia arbitraria. Se amparó a los condenados declarando ilícita la intervención telefónica del teléfono de la víctima que obraba en poder de los detenidos y que se realizó en dependencias policiales mientras estaban detenidos.
9. Casos Fernández Saavedra c. España (2010) o Abdulkadir Coban c. España (2006), entre otros.
10. STJUE, de 8 de abril de 2014 (asunto Digital Rights) y de 21 de diciembre de 2016 (asunto Tele2 Sverige).
11. Las cuestiones que se estimaban a tal efecto eran la falta de determinación de las condiciones materiales y de procedimiento (pgf. 61), y la falta de información al usuario del hecho de la conservación de los datos (pgf. 39); la falta de la delimitación de los criterios objetivos de acceso y, concretamente, la falta de control jurisdiccional previo (pgf. 62); la falta de discriminación de los criterios temporales para la conservación de los datos, así como la falta de criterios objetivos en orden a garantizar que esta se limite a lo estrictamente necesario (pgf. 64); y la falta de garantía en orden a la seguridad y conservación de los datos, principalmente por la intervención de una autoridad independiente (pgf. 68) y la falta de control de los datos en caso de cesión de los mismos fuera del territorio de la Unión. Retengamos estos motivos para el examen posterior de la «cuestión prejudicial» planteada respecto a la regulación nacional contenida en la reforma de 2015, pendiente de resolución en el TJUE y a la que nos referiremos después.
12. Rodríguez Lainz (2017), a cuyo juicio, no sólo hay que reformar la Ley de Conversión de datos, sino también la Ley de Enjuiciamiento Criminal. En igual sentido se pronuncia I. M. Colomer Hernández (2017).
13. A juicio de Rodriguez Lainz (2014) y Colomer Hernandez (2017), las nuevas exigencias para autorizar judicialmente la cesión de esta clase de datos, orientadas a comprobar que la retención y conservación de los mismos respetan los nuevos límites de respeto a los derechos humanos, obligan a que el legislador modifique el texto a tenor de los nuevos parámetros: con criterios de limitación temporal, de finalidad y de no sujeción indiferenciada de todos los usuarios, estableciendo un régimen de retención y conservación preventiva de estos datos de tráfico y localización que permita su cesión.
14. Los artículos 579 a 588 integraron un nuevo capítulo III del título VIII del libro II que otorgó un nuevo y pormenorizado contenido a las «medidas de investigación tecnológicas». Una explicación pormenorizada del alcance y extensión de estos presupuestos que operan como «principios rectores» en Armenta Deu (2017, pág. 72-74, 183-185 y 195-200).

para obtener los datos que pueden alojar, cabe acudir al «acceso y registro para aprehender los datos relevantes contenidos en los mismos, y a la orden de entrega a los depositarios de esos datos», si se trata de información retenida en poder de terceros.[15]

Del conjunto de medidas posibles serán algunas de las contempladas en el apartado a) las que centren nuestra atención; concretamente las de interceptación encaminadas a captar el contenido de la comunicación intervenida junto con los datos de tráfico, que como elementos del proceso comunicativo gozan de la protección del derecho al secreto de las comunicaciones (art. 18.3 CE).[16] Cuestión distinta, y que no se abordará, será la observación, encaminada tan solo a determinar la procedencia e identidad de los interlocutores o alguno de esos datos de tráfico anexos al proceso comunicativo, medidas de registro de sistemas y dispositivos informáticos o de cesión de datos y archivos informáticos, entre otras.

4. Valor probatorio de los correos electrónicos, mensajes de WhatsApp, Twitter, Instagram y otras redes sociales. Doctrina y jurisprudencia tras la reforma 2015

En la prueba electrónica cabe diferenciar dos modalidades: a) los datos o informaciones almacenados en un dispositivo electrónico (incluyendo sistemas informáticos y cualquier aparato informático o de tecnología digital, como los medios de almacenamiento masivo); y b) los que son trasmitidos por cualquier red de comunicación abierta (internet, telefonía fija o móvil) o restringida, o a través de una red de comunicación en la que no existe comunicación entre personas determinadas o determinables. Ante la imposibilidad de analizarlas de manera individualizada, centraré mi atención en las principales formas de fuentes de prueba digital por corresponder a aquellas que han suscitado mayor debate doctrinal y jurisprudencial.[17]

4.1. Correo electrónico

Compuesto del contenido del mensaje junto a sus anexos (texto, imagen, vídeo) y de los datos de tráfico (fecha, hora, duración, origen y destino), una definición adecuada es la contenida en el artículo 2 h) de la Directiva 58/2002/CE, de 12 de julio.[18] La acreditación de un *mail* puede efectuarse mediante cualquiera de los dispositivos electrónicos de remisión o recepción, y/o en cualquiera de los servidores implicados, si bien la facilidad de acceso, según la empresa operadora tenga su sede o no en España y la eficacia probatoria de cada uno varía.[19] Con todo, resultará más sencillo probar el contenido del mensaje mediante el acceso a los dispositivos electrónicos utilizados para la comunicación por el emisor o el receptor del mail.

Teniendo presente que afectará al derecho fundamental a la intimidad y/o al secreto de las comunicaciones, según el acceso al correo electrónico tenga lugar con anterioridad a iniciar el proceso de comunicación o no sea así, y

15. Cabezudo Rodríguez (2016).
16. Como es conocido, la medida de intervención puede recaer sobre: 1) el contenido del acto de comunicación; 2) los denominados datos de tráfico (origen de la comunicación, el destino, la ruta, el tiempo, la fecha, el tamaño, la duración del tipo de servicio, art. 1 del Convenio sobre Cibercrimen); 3) o la información personal del usuario o abonado que supuestamente efectúa la transmisión. Mediante tales medidas se reconoce sustantividad propia a la interceptación telefónica y telemática (Marchena Gómez y González-Cuellar Serrano, 2015, pág. 201).
17. Se sigue la opción de Delgado Martín (*op. cit*, cap. 3).
18. Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que señala: «Todo mensaje de texto, voz o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que este acceda al mismo».
19. La conservación de los datos tendrá presente el cumplimiento de las obligaciones de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, si se trata de datos conservados por las entidades prestadoras de servicios; del artículo 588 ter j LECrim, cuando sean datos conservados por la operadora que no sean en cumplimiento de la ley citada anteriormente; del artículo 11.2 d) LO de protección de datos, cuando sean datos conservados por la compañía a iniciativa propia; o el caso contemplado en el artículo 588 ter LECrim.

según se trate de los datos de cabecera o el contenido del mensaje,[20] la injerencia deberá:

- cumplir los presupuestos de las medidas limitativas de derechos fundamentales;[21]
- aportarse al proceso mediante un medio probatorio adecuado: en formato papel, como documento electrónico;[22] y a través de copia del disco duro o del disco duro del servidor al que llegó el correo electrónico, con su correspondiente *código hash* calculado ante fedatario público;[23] acompañándose del correspondiente informe, cuyas conclusiones podrán incorporarse mediante prueba pericial;[24] o recurriendo a algún «prestador de servicio de confianza», conforme a lo dispuesto en el Reglamento UE/910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior;[25]
- salvaguardar la cadena de custodia (arts. 777.2,1,II y III LECrim), y
- reproducirse correctamente en el juicio (art. 797,2,1,II y III LECrim).

Cuestión diferente será la valoración que corresponda a cada uno de los medios probatorios y la eventual valoración conjunta, aplicando las reglas de la sana crítica, o lo que es igual, el principio de libre valoración (art. 741 LECrim) y el resultado final. Aspectos que dependen, a su vez, del medio probatorio incorporado al proceso, su autenticidad y la postura procesal de las partes. Así, por ejemplo, la utilización como prueba del documento electrónico, a falta de norma específica en la Ley de enjuiciamiento criminal, se adecuará a lo dispuesto en el artículo 230.1 LOPJ, Ley 59/2003, artículo 3 de la Firma electrónica, y artículo 299.2 LEC, por analogía, conforme a lo dispuesto en el artículo 4 LEC;[26] en tanto a la prueba electrónica de documentos públicos y de documentos oficiales corresponde, también por analogía, la valoración establecida en el artículo 319.1 y 2 LEC, ya que los documentos electrónicos privados deben pasar el filtro de la autenticidad e integridad de los datos a través de la llamada «copia forense».[27]

La impugnación de la autenticidad o integridad por alguna de las partes revertirá en la necesidad de acreditar los hechos mediante otro medio probatorio, que atendidas las complejidades técnicas suele ser la pericia,[28] aunque no solo.[29]

20. Si el mensaje se redacta y no sale del dispositivo afecta sólo al derecho a la intimidad, pero desde el momento en que sale (este en curso o almacenado en el servidor de la operadora) ya afectaría también al secreto de las comunicaciones; es decir, como acontece con el acceso a un mensaje después de su envío por el remitente cuando está en proceso de transferencia hasta el destinatario, debiendo efectuarse conforme a las prescripciones del art. 588 ter a y ss LECrim; o cuando se trata de un mail que todavía no ha leído su destinatario y está almacenado por la operadora.
21. Artículo 588 bis a) a artículo 588 bis k LECrim. STS 877/2014, de 22 de diciembre.
22. Previa clonación del disco duro ante LAJ o notario, elaborando posteriormente un informe de experto que podrá presentarse en el proceso mediante el correspondiente peritaje. Rubio Alamillo (2016). STS 298/2015, de 13 mayo.
23. Pereira Puigvert (2013); Bueno de Mata (2016a, pág. 248 y ss).
24. El informe pericial informático (de técnicos especialistas) sirve para afianzar el valor probatorio de un correo electrónico mediante el análisis del equipo o equipos que lo contiene, los datos de cabecera y sobre todo su correspondencia cronológica. Martínez Carvajal Hedrich (2013).
25. Reglamento (UE) núm. 910/2014, del Parlamento Europeo.
26. A los «pantallazos» obtenidos del teléfono móvil se les niega valor de documento, entendiendo que se trata de una prueba personal documentada posteriormente para su incorporación a la causa (STS 300/2015, de 19 de mayo; negativa que ya se predicaba de las trascripciones de diálogos o conversaciones mantenidas por teléfono (SSTS 1024/2007, 1157/2000 o 942/2000). Negativa que se extiende a los pantallazos de Facebook (STS 782/2016, de 16 de octubre).
27. Captura de todos los datos de la fuente de evidencia electrónica para que permanezca inalterada; e informe pericial por unidades policiales especializadas o peritos informáticos no públicos. El código *hash* es el principal instrumento técnico al efecto. Delgado (*op. cit*., cap. I, pág. 14), y Pereira Puigvert, *op. cit*.
28. Sobre la relevancia de la pericia en este ámbito, Rodríguez Lainz (2015, *op. cit*., y nota 52).
29. En el caso resuelto por la STS 300/2015, de 19 de mayo, se aprecia la autenticidad de un diálogo mantenido a través de Tuenti entre la víctima de abusos sexuales y un amigo al que relata varios incidentes, y que constituye prueba suficiente de cargo, por dos razones: que la propia víctima fue quien puso a disposición del juez su contraseña de Tuenti por si esta era puesta en duda, como ocurrió; y que el interlocutor fuera propuesto como testigo acudiendo al plenario y pudiendo ser interrogado por las acusaciones y la defensa, corroborando que tal conversación se mantuvo. Un juicio crítico en De Bueno Mata (2016b).

4.2. WhatsApp y otros sistemas de mensajería instantánea

Las especiales características de esta forma de comunicación entre usuarios mediante una aplicación para teléfonos móviles y *smartphones* que permite enviar mensajes de texto, notas de audio y vídeo, compartir contactos o la propia ubicación presentan algunas diferencias con el correo electrónico y SMS, ya que la información transmitida no se conserva por un servidor externo, se utilizan protocolos de seguridad para garantizar el cifrado de la información[30] y resulta disponible en multiplataforma: IOS, Android, Windows Phone. El hecho de que el contenido no quede almacenado en el servidor del administrador impide que la autoridad judicial pueda solicitar a la empresa prestadora del servicio que certifique el contenido de mensajes enviados o recibidos, teniendo que acudirse a los dispositivos electrónicos usados para su conversación.[31] Cuestión diferente será la de los datos de tráfico generados durante la conservación de WhatsApp y que no constituyen contenido de la conversación (origen y destino, ruta, hora, tamaño y duración de la comunicación).[32]

Como en los restantes medios analizados, el enorme riesgo de manipulación o de generación de mensajería instantánea, suplantación de origen o de identidad[33] condujo a diversos pronunciamientos que recalcaban la importancia del medio de aportación al proceso y del análisis pericial de los datos examinados respecto de comunicaciones cuya realidad o autenticidad se cuestiona,[34] así como a la necesidad del análisis detenido de los correspondientes terminales, si es posible entre supuestos emisor y receptor, así como que no haya sido manipulado.[35]

A lo largo de varias resoluciones se estableció una «regla de carga probatoria» que desplazaba a quien aportara o a quien pretende valerse de su valor probatorio acreditar el verdadero origen de la comunicación, identidad de los interlocutores y la integridad de su contenido.[36] Con todo, el rigor de este desplazamiento de la carga probatoria se fue matizando notablemente, de manera que si bien resulta taxativa respecto de los llamados «pantallazos» o simples impresiones de concretas comunicaciones o de su rastro,[37] en cuanto al resto –aportación mediante soportes electrónicos originales o copia, o acompañando el original– se apela a un examen singularizado y cauteloso.[38]

Si quisiéramos elaborar una sucesión esquemática de los pasos a seguir en la valoración, transcurriría así:

- la aportación del original otorga mayor facilidad probatoria a cualquier copia o «pantallazo», al igual que la falta de impugnación puede ser valorada como aceptación tácita de su autenticidad y validez;

- cuando se impugne la autenticidad, corresponde a quien la ha aportado reforzar aquella, lo que generalmente se llevará a cabo mediante la prueba pericial. Pericia que, por su parte, siendo como es un medio probatorio idóneo por las especificidades técnicas que concurren, no constituye, empero, un medio incontestable, ya que puede depender a su vez de circunstancias ajenas a la propia pericia y del buen quehacer del mismo perito o incluso de la concreta pericia del caso.[39]

Ahora bien, ni la simple impugnación desvirtuará el valor probatorio, en todo caso, ni su resultado tendrán un efecto determinante. La valoración, como es conocido, la lleva a

30. Rodríguez Lainz (2015); Arrabal Platero (2017.
31. García Mescua (2018).
32. Dicha información, útil eventualmente para el proceso penal, podrá ser reclamada si se conserva por la operadora.
33. Una amplia y pormenorizada descripción de los posibles métodos y niveles de intrusión, así como de las eventuales técnicas forenses de detección del fraude en el trabajo de Rodríguez Lainz (2015) y en De Bueno Mata, *op. cit*.
34. STS 342/2013, de 17 de abril y notas 30 y 52.
35. La investigación se centrará en la memoria interna del terminal, volcar la presencia de códigos propios de esos terminales, dirección IP del servidor que reenvía los datos, en su caso y otros aspectos que figuran en las tarjetas de memoria SD (Delgado Martín, 2016, *op. cit*., cap. 3).
36. STS 300/2015, de 19 de mayo.
37. Representaciones en papel impreso de copias de pantalla o pretendidas comunicaciones emitidas y/o recibidas por quien las aporta o por alguien que las ha facilitado a las que se niega valor probatorio *per se*. Sentencias citadas en nota 26.
38. STS 300/2015, de 19 mayo; 298/2015, 13 de mayo; y 786/2015, 4 de diciembre.
39. Así por ejemplo, que pueda acceder a la fuente original o no sea así; que se pueda cotejar la realidad de la existencia de la comunicación, su recepción y la coincidencia de las versiones. Sin rechazar que pueda variar la misma calidad de los conocimientos y medios empleados por el perito. *Cfr*. Rodríguez Lainz (2003, pág. 391-396).

cabo el juez con arreglo a las reglas de la sana crítica, contrastando todos los medios probatorios, lícitos, admitidos y practicados conforme a las garantías probatorias,[40] de forma que tanto la valoración conjunta con otros medios probatorios puede conducir a que la pretendida falta de autenticidad quede contradicha por otros medios, como que se ratifique el contenido por parte de los interlocutores o el testimonio de la testigo denunciante,[41] que se facilite el acceso a la fuente original[42] o que se suscite contradicciones entre lo declarado por el acusado.[43]

4.3 Redes sociales y otros elementos web

Del inabarcable mundo de las redes sociales[44] me centraré en el hecho de que cada usuario construya un perfil público o semipúblico en un sistema delimitado o cerrado y en que se elabora una lista de otros usuarios que comparten relaciones, pudiendo recorrerse la lista de relaciones que las personas tienen con otras del sistema.[45]

Entre las múltiples consecuencias jurídicas que implica este quehacer, presenta relevancia probatoria la información obtenida de las redes sociales y la prueba de los hechos delictivos cometidos en las mismas.[46] En el primer sentido, la investigación de los hechos requerirá fuentes y medios clásicos y novedosos orientados a investigar la huella digital, la autoría y/o la localización de la empresa prestadora del servicio. Por lo que hace a la información obtenida en las redes sociales, se orientará a analizar el rastro digital, tanto para investigar un ilícito cometido en la red como fuera de ellas. La titularidad de la cuenta puede ser también el objeto de investigación, lo que se hará averiguando la dirección IP utilizada para colgar el contenido ilícito y, a partir de ahí, la cesión de datos de identificación y localización del dispositivo, identificación que precisará de autorización judicial (art. 588 ter k LECrim).[47]

A falta de un precepto que regule la aportación de fuentes de prueba de estas características,[48] cabrá que el Ministerio Fiscal o las partes proporcionen información contenida en las redes sociales, tanto de perfiles propios como ajenos a cuyo contenido se pueda acceder lícitamente, así, la información insertada voluntariamente en la red para ser compartida con otros usuarios no goza de la protección del secreto de las comunicaciones; sin embargo, la amplitud de actividades obligará a un examen más concreto, en supuestos como la información trasmitida entre un grupo limitado o identificado de interlocutores, ámbito en el que sí resultaría aplicable el artículo 18.3 CE. Otro medio de aportación es a través de la información almacenada en un servidor, aspecto este que cuando –como es frecuente– se trata de servidores que tienen su sede fuera del territorio español, genera no pocos problemas cuya eventual solución discurre a través de la cooperación

40. En el caso de ilicitud probatoria, cabe haber excluido la fuente probatoria, pero también es posible que sea el momento de la valoración cuando el juez tiene todos los elementos para discernir sobre la concurrencia de infracciones al derecho fundamental que determinen que no puede ser objeto de valoración (Armenta Deu, 2011, pág. 141-143).
41. Sentencia 702/2015, de 24 de noviembre, de la Sección 27.ª de la AP de MD.
42. La simple aceptación o no impugnación propició su valoración probatoria en SSTS 899/2014, de 26 de diciembre (WhatsApp entre víctima de malos tratos y un amigo en donde narraba la situación); 126/2015, de 12 de mayo; 258/2015, de 8 de mayo (conversaciones a través de chats con un menor de edad para proponerle relaciones sexuales); 264/2015, de 7 de mayo; 298/2015, de 13 de mayo; o 515/2013, de 13 junio.
43. Así por ejemplo, en un caso en que se pretendía la valoración de un hecho como incontestable de un «pantallazo» de Facebook en donde la menor se aumentaba la edad, la Sala valoró la contradicción sobre ese dato, ante el juez de instrucción, donde admitió conocer la edad de la víctima, y el plenario cuando lo negó (STS 782/2016, de 15 de octubre).
44. Información generada en las web horizontal (con carácter generalista) y vertical (dirigida a usuarios con perfil específico y predefinido); redes de difusión de conocimiento (aquellas en cuyos servicios a través de internet cuenta con personas con intereses comunes que interactúan en igualdad de condiciones); o redes sociales: directas, que suelen carecer de usuarios con perfil visible para todos, existiendo alguien que controla y dirige las discusiones en un tema concreto (foros, blogs, etc.) (Davara Fernández de Marcos, 2015, *passim*).
45. Agustinoy Guilayn y Monclús Ruiz (2016).
46. Se sigue en esta exposición el orden de Delgado Martín (op. cit, cap. 3).
47. Sobre los pantallazos, como instrumento habitual de incorporar el texto del correo electrónico, destacan su escaso valor *per se*, y la necesidad de acompañarlos del correspondiente informe pericial, para demostrar la autenticidad de las conversaciones, así como del uso de la red social Tuenti, STS 300/2015, de 19 de mayo, 281/2016, de 14 de septiembre, así como las resoluciones que figuran en la nota 28. También: Rodríguez Lainz (2015, *op. cit*.)
48. La única excepción, y con el carácter específico que le otorga su ámbito de aplicación, es el artículo 11 b) Ley 4/2015 de 27 de abril, del estatuto de la víctima del delito.

judicial internacional,[49] ya sea mediante la aplicación del Convenio de Budapest, para países fuera de la UE,[50] y en el marco comunitario, el Convenio de 29 de mayo, de asistencia judicial en materia penal entre los miembros de la Unión Europea, la Directiva 2014/41/CE, Orden Europea de Investigación penal,[51] y en aquello no comprendido por la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE.

En lo relativo a la valoración probatoria, cabe recordar lo hasta ahora expuesto en un doble plano: 1.º) que las distintas informaciones insertas en el perfil abierto son colgadas libremente, por lo que difícilmente afectarán al derecho a la intimidad; y 2.º) que en caso de limitar algún derecho fundamental, como el sitio web de acceso restringido a un grupo cerrado de personas, la valoración del medio probatorio aportado (documento, inspección ocular, pericia, testimonio o interrogatorio de parte o del acusado) debería superar un doble control: que la fuente ha sido obtenida salvaguardando rigurosamente los requisitos contemplados en los artículos 588 bis LECrim (con carácter general) y lo dispuesto en el artículo 588 ter LECrim, en particular, así como que ha sido incorporada al proceso y en su caso reproducidas en el juicio oral con las debidas garantías de audiencia y contradicción.[52] De otra forma, la ilicitud probatoria, si no provocó su exclusión por no resultar lo más procedente,[53] no podría enervar la presunción de inocencia; efecto similar al que se ocasionaría, aun no tratándose de una fuente de prueba ilícitamente obtenida, en el caso de cualquier medio de prueba que no cumpla con los requisitos comprendidos en el derecho a utilizar todos los medios pertinentes para la defensa y a la presunción de inocencia.[54]

5. La incertidumbre tras la cuestión de prejudicialidad (Asunto C-207/16)

En este contexto, y mediante auto de la AP de Tarragona, el 14 de abril de 2016, se instó una «cuestión prejudicial ante el TSJUE» solicitando un pronunciamiento sobre los artículos 579 y 588bis LECrim –donde se definen los presupuestos que autorizan la injerencia del Estado en las comunicaciones telemáticas de los sospechosos– por si pudieran ser contrarios a los principios y derechos de la Unión (arts. 7 y 8 CDFUE y 8 CEDH).[55] Se destaca, en apretada síntesis, que la injerencia de intensa lesión para los derechos fundamentales afectados se efectúa mediante una fórmula que define el umbral penológico de manera tal que no satisfacen la exigencia de proporcionalidad requerida por el derecho de la Unión Europea, especialmente en cuanto a la delimitación del estándar de gravedad que justifica dicha injerencia. En otros términos, se cuestiona el criterio de «gravedad suficiente» identificado únicamente por la pena que pueda imponerse al delito que se investiga, sin concretar en la conducta particular nivel de lesividad para bienes jurídicos individuales o colectivos; y asimismo, en caso de que sí se ajustara, se pregunta cuál debería ser el nivel mínimo de la pena imponible, cuestionando si este es compatible con una previsión general de límite de tres años de prisión, como se contempla en los artículos 579 y 588 bis, ambos de la LECrim. Fuente confesada de este planteamiento es la STJUE de 8 de abril de 2014, a cuyos fundamentos 46 a 48, 52, y 53 y siguientes nos remitimos[56] en espera de la resolución a la citada Cuestión.[57]

49. Art. 276 LOPJ.
50. Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, ratificado por España en 2010 (BOE de 17 de septiembre de 2010) y aplicable para cualquier proceso penal en orden a obtener pruebas electrónicas de los delitos (art. 23).
51. Cuyo artículo 3 extiende la posibilidad de emitir una OEI a todos los medios de prueba, excepto la creación de un «equipo conjunto de investigación», extendiéndose incluso a medios diferentes a los de la OEI en los supuestos del artículo 10, a excepción de la identificación de personas que sean titulares de un número de teléfono o una dirección IP determinados, en cuyo supuesto se requiere que tal medida esté contemplada en el Estado de ejecución (art. 10, 2, e).
52. Recuérdese aquí lo expuesto respecto al modo de incorporación al proceso y la relevancia de la prueba pericial técnica, es decir, la efectuada por un perito cualificado en aspectos informáticos. Al respecto, Sáez-Santurtún Prieto (2105) y Martínez Carvajal Hedrich (2013).
53. Sobre el momento de apreciación: STS 255/2017, de 6 de marzo y 85/2017, de 15 de febrero.
54. Nota 40, y en particular, Sáez-Saturtún Prieto (2015).
55. Accesible en ‹http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62016CN0207&from=ES›.
56. *Vid.* nota 12. Adviértanse las similitudes en cuanto a discriminación de criterios temporales o falta de criterios objetivos para garantizar una limitación estrictamente necesaria, por ejemplo.
57. Enviado el trabajo y en periodo de revisión se han publicado las «Conclusiones del Abogado General» (3 de mayo de 2018). Atendiendo a que,

6. Reflexión final

Las medidas tecnológicas utilizadas a la hora de obtener la fuente de prueba digital pueden resultar muy invasivas, generando importantes riesgos de vulneración de derechos fundamentales; en este ámbito se abre un importante interrogante en función de la resolución que obtenga la cuestión prejudicial pendiente de resolución por el TJUE. Paralelamente, por su complejidad y volatilidad, requieren adecuar la regulación de la prueba en sus diferentes fases: obtención, incorporación al proceso y valoración; aspecto conexo con el anterior y que obliga a un nuevo esfuerzo legislativo que dé respuesta a las deficiencias señaladas en este y otros análisis.

Con todo, y sin restar importancia al tema central de este trabajo, las complejidades de la prueba digital no pueden empañar que, a la postre, la valoración probatoria se proyectará en primer lugar sobre la calificación de la validez y licitud de la fuente correspondiente, y en segundo lugar, sobre la ponderación de la eficacia o fuerza convincente del conjunto de medios, según las reglas de la sana crítica; de manera que solo la garantía de ambos extremos enerva válidamente la presunción de inocencia.[58] Las seis vertientes: condenar con suficientes pruebas de cargo; con base en pruebas lícitas; motivando la convicción probatoria; sobre la base de pruebas suficientes; o sobre la base de una motivación lógica, irregular o concluyente, aunque no conformen compartimentos estancos, deben ser respetadas para alcanzar una condena como contenido primario del autónomo derecho a un proceso con todas las garantías (art. 24.2 CE).[59]

Bibliografía citada o recomendada

AA. VV. (2017). *Justicia Penal y nuevas formas de delincuencia,* J. M. ASENCIO MELLADO(dir.). M. FERNÁNDEZ LÓPEZ (coord.). Tirant lo Blanch.

AA. VV. (2017). *Fodertics 6.0 7) Los nuevos retos del derecho ante la era digital-*. F. BUENO DE MATA (dir.). Comares.

AA. VV. (febrero 2017). «La Sentencia del TJUE de 21 de diciembre de 2016, que declara contraria al Derecho de la UE una ley que regule la conservación de datos, ¿en qué grado afecta a la Ley 25/2007, de 18 de octubre, y a la reciente reforma de la LECrim., en lo que a la cesión de datos se refiere, respecto a la investigación de delitos cometidos a través de Internet?» *Sepin, Encuesta Jurídica*.

AGUSTINOY GUILAYN, A.; MONCLÚS RUIZ, J., (2016). «Aspectos legales de las redes sociales». Bosch.

ARMENTA DEU, T. (2017). «Lecciones de derecho procesal». 10ª edición, Marcial Pons.

ARMENTA DEU, T. (2014). «Limitación de derechos fundamentales y prueba ilícita» En: *Estudios de Justicia Penal*. Marcial Pons.

ARMENTA DEU, T (2011). «La prueba ilícita. Un estudio comparado». 2ª ed., Marcial Pons.

ASENCIO MELLADO, J. M.; FERNÁNDEZ LOPEZ (2017). «Justicia penal y nuevas formas de delincuencia». Ed. de la Universidad de Alicante.

ARRABAL PLATERO, P. (2017). «El WhatsApp como fuente de prueba». En: O. FUERTES (cood.). *El proceso penal: cuestiones fundamentales*. Valencia: Tirant lo Blanch.

pese a su relevancia y a que suelen ser ciertamente un adelanto del sentido del fallo posterior, la limitación de la extensión del trabajo, de un lado, y sobre todo, de otro, la prudencia, aconsejan dejar para un posterior comentario no solo dichas Conclusiones, sino el fallo final, que al fin y al cabo depende del criterio de los magistrados.

58. STC 33/2002; STS 653/2016, de 18 de julio, F.J. n.º 21 y antes: STS 255/2017, de 6 de marzo, F. J. n.º 7. SSTC 109/1986, 68/1988 y, entre otras muchas, 207/2007 y 145/2014.

59. STS 255/2017, de 6 de marzo, F.J. n.º 8 y STS 675/ 2015, de 10 de noviembre y 250/2017, F.J, n.º 6.

BUENO DE MATA, F. (2016a). «Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de WhatsApp, Snapchat o Telegram». En: AA. VV., «Hacia una justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e informática». Salamanca: Ratio Legis.

BUENO DE MATA, F. (2016b). «La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica». *Diario la Ley*, nº 8728, 23 de marzo.

BUENO DE MATA, F. (2016c). «La validez de los "screenshots o "pantallazos" como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo». En: A. M. NEIRA PENA (dir.). F., BUENO MATA y J. PEREZ GIL (coord.). «Los desafíos de la justicia en la era post crisis». Atelier.

CABEZUDO RODRÍGUEZ, N. (2016). «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal». *BMJ*, año LXX, número 2186, febrero.

CASTILLEJO MANZANARES, R. (2010). «La prueba en el proceso penal: el documento electrónico». *Revista de Derecho Penal*, n.º 29.

DAVARA FERNÁNDEZ DE MARCOS, L. (2015). «Implicaciones Socio-Jurídicas de las Redes Sociales». Thomson Reuters Aranzadi.

DELGADO MARTÍN, J. (2016). «Investigación tecnológica y prueba digital en todas las jurisdicciones». *La Ley*, ed. digital.

DELGADO MARTÍN, J. (2017). «La prueba electrónica en el proceso penal». *Diario La Ley*, n.º 8167.

ENCINAR DEL POZO, M. A.; VILLEGAS GARCÍA (2017). «Validez de medios de prueba tecnológicos». *Diario la Ley*, n.º 9005, 21 de junio.

FUENTES SORIANO, O. (2017). «Comunicaciones telemáticas: práctica y valoración de la prueba». AA. VV. *El proceso penal: cuestiones fundamentales*. Tirant lo Blanch.

GALLEGO SÁNCHEZ, G. (2010). «Sobre el secreto de las comunicaciones, el art. 579 LECrim y las intervenciones telefónicas». *El Derecho. com,* <http://www.elderecho.com/tribuna/penal/secreto-comunicaciones-LECrim-intervenciones-telefonicas_11_159055012.html>

GARCÍA MESCUA, D. (2018). *Aportación de mensajes de WhatsApp a los procesos judiciales. Tratamiento procesal.* Comares.

GARRIDO CARRILLO, F. J. (2013-2014). «La prueba electrónica en los procesos civiles y penales». *Revista de la Facultad de Derecho de la Universidad de Granada*, n.º 16-17.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E. (2017). «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, n.º 125.

MAGRO SERVET, V. (2006). «La prueba pericial informática. La utilización de los medios de prueba informáticos en el proceso penal». *La Ley Penal*, n.º 33.

MARCHENA GÓMEZ, M.; GONZÁLEZ-CUÉLLAR SERRANO, N. (2015). *La reforma de la Ley de Enjuiciamiento Criminal en 2015.* Castillo de Luna, Ediciones Jurídicas.

MARTÍNEZ CARVAJAL HEDRICH, E. (2013). «Valor probatorio de un correo electrónico». *Diario La Ley*, n.º 8014, febrero.

PINTO PALACIOS, F.; PUYOL CAPILLA, P. (2017). «La prueba en la era digital». *La Ley*. Wolters Kluwer.

PEREIRA PUIGVERT, S. (2013). *La exhibición de documentos y soportes informáticos en el proceso civil*. Thomson Reuters-Aranzadi.

PORTAL MANRUBIA, J. (2013). «La regulación de la prueba electrónica en el proceso penal». *Revista de Derecho y Proceso Penal*, n.º 31.

RODRÍGUEZ LAINZ, J. L. (2015). «Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2ª, 300/2015, de 19 de mayo)». *Diario la Ley*, n.º 8569, sección doctrina, 25 de junio de 2015.

RODRÍGUEZ LAINZ, J. L. (2014). «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la Ley española sobre conservación de datos relativos a las comunicaciones». *La Ley*, n.º 8308.

RODRÍGUEZ LAINZ, J. L. (2003). *Intervención judicial en los datos de tráfico de telecomunicaciones electrónicas*. Bosch.

RODRÍGUEZ LAINZ, J. L. (2017). «La jurisprudencia del tribunal de Luxemburgo sobre regímenes de conservación preventiva de datos en la Doctrina del Tribunal Supremo». *Diario La Ley*, nº 9087.

RUBIO ALAMILLO, J. (2016). «El correo electrónico como prueba en procedimientos judiciales». *Diario la Ley*, n.º 8808, Sección Práctica Forense 21 de julio de 2016.

SÁEZ-SANTURTÚN PRIETO (2105). «La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 de mayo de 2015». *Diario la Ley*, n.º 8637.

URBANO CASTRILLO, E. (2011). «La regulación legal de la prueba electrónica: una necesidad pendiente». *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*. n.º 82.

VERVAELE, J., (2012). «Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal». En: «El proceso penal en la sociedad de la información». *La Ley*.

Cita recomendada

ARMENTA DEU, Teresa (2018). «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, whatsapp, redes sociales): entre la insuficiencia y la incertidumbre». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 67-79. UOC [Fecha de consulta: dd/mm/aa]
‹http://dx.doi.org/10.7238/idp.v0i27.3149›

Sobre la autora
Teresa Armenta Deu
teresa.armenta@udg.edu

Catedrática de Derecho Procesal
Universitat de Girona

http://www2.udg.edu/professorat/Planapersonal/tabid/8656/ID/51892/language/es-ES/Default.aspx

Facultat de Dret
Campus Montilivi
17003 - GIRONA
Despatx: 219