PROCESSO PENALE
e POLITICA CRIMINALE

Collana diretta da

G. Paolozzi - S. Moccia - L. Marafioti
L. Lupária - P. Marchetti - N. Selvaggi

14

pea dei diritti dell'uomo. La Corte ha detto chiaramente che la qualità delle fattispecie limitative del diritto alla vita privata, la loro chiarezza e precisione, il livello di dettaglio possono e devono variare in relazione al grado di intrusività della misura adottata. Più lo strumento è invasivo – e un captatore informatico è incomparabilmente più invasivo di una microspia –, più la previsione dei casi, dei modi e delle garanzie deve farsi chiara, precisa e dettagliata.

Tutto questo rendeva comunque necessario l'aggiornamento legislativo della disciplina dell'intercettazione, con buona pace della sua asserita "neutralità tecnica", cioè della sua pretesa indifferenza alla tipologia degli strumenti tecnologici utilizzati per l'ascolto. Il legislatore ci ha finalmente provato con la riforma Orlando: ma gli incerti destini della riforma – e l'esaurirsi del tempo a mia disposizione – suggeriscono di rinviare a un'altra occasione l'analisi dei suoi contenuti.

Capitolo III

Algunas consideraciones sobre la valoración probatoria de fuentes de prueba digital (correos electrónicos, *Whatsapp*, redes sociales): perspectivas española y europea*

Teresa Armenta Deu

SUMARIO: 1. Introducción: consideraciones generales. – 2. La situación hasta 2015: carencias normativas e interpretación jurisprudencial. – 3. La reforma de 2015. – 4. Valor probatorio de los correos electrónicos, mensajes de *Whatsapp*, *Twitter*, *Instagram* y otras redes sociales. Doctrina y jurisprudencia tras la reforma 2015. – 4.1. Correo electrónico. – 4.2. *Whatsapp* y otros sistemas de mensajería instantánea. – 4.3. Redes Sociales y otros elementos *web*. – 5. La incertidumbre tras la "cuestión de prejudicialidad (Asunto C-207/16). – 6. La Sentencia del Tribunal de Justicia (Gran Sala), de 2 de octubre de 2018. – 7. Las futuras órdenes europeas de entrega y conservación de pruebas penales electrónicas. – 8. Algunas reflexiones finales.

1. *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

---

*Este trabajo tuvo su origen en mi artículo «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, *Whatsapp*, redes sociales): entre la insuficiencia y la incertidumbre», en A. GONZÁLEZ JIMÉNEZ (coord.), *Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes*, en *IDP. Revista de Internet, Derecho y Política*, n. 27, pp. 67-79; habiendo sido revisado y ampliado tras la celebración del Congreso "Dimensione tecnologica e prova penale" del que trae causa la presente publicación.

Ambos trabajos han sido realizados 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).

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 sólo 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 de prueba o de la prueba tecnológica[5], eximen de analizar algunos aspectos, pero no de situar al lector

[1] Las nuevas tecnologías en el enjuiciamiento penal ofrecen un doble enfoque: como objeto y como instrumento. J. DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, en *La Ley*, 2016, edición, digital, capítulo, I, y nota 5.

[2] J.M. ASENCIO MELLADO-M FERNÁNDEZ LÓPEZ, *Justicia penal y nuevas formas de delincuencia*, ed. Tirant lo Blanch, Valencia, 2017.

[3] N. CABEZUDO RODRIGUEZ, *Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento en la Ley de Enjuiciamiento Criminal*, en *BMJ*, año LXX, número 2186, febrero 2016, p. 9.

[4] Desde el 11S, el atentado en Londres y el 5M 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. T. ARMENTA DEU, *Limitación de derechos fundamentales y prueba ilícita*, en *Estudios de Justicia Penal*, Marcial Pons, Madrid, 2014, pp. 229-252. J. DELGADO MARTIN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, cit., capítulo II.

[5] A título indicativo: F. BUENO DE MATA, Fodertics 6.0: *Los nuevos retos del derecho ante la era digital*, Comares, 2017; V. MAGRO SERVET, *La prueba pericial informática. La utilización de los medios de prueba informáticos en el proceso penal*, en *La Ley Penal*, n. 33, 2006, pp. 107-115; R. CASTILLEJO MANZANARES, *La prueba en el proceso penal: el documento electrónico*, en *Revista de Derecho Penal*, n. 29, 2010, pp. 11-43; E. URBANO CASTRILLO, *La regulación legal de la prueba electrónica: una necesidad pendiente*, en *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, n. 82, 2011; J. DELGADO MARTÍN, *La prueba electrónica en el proceso penal*, en *Diario La Ley*, n. 8167; J. PORTAL MANRUBIA, *La regulación de la prueba electrónica en el proceso penal*, en *Revista de Derecho y Proceso Penal*, n. 31, 2013, pp. 19-41; F.J. GARRIDO CARRILLO, *La prueba electrónica en los procesos civiles y penales*, en *Revista de la Facultad de Derecho de la Universidad de Granada*, n. 16-17, 2013-2014, pp. 553-590; F. PINTO PALACIOS-P. PUYOL CAPILLA, *La prueba en la era digital*, Wolters Kluwer La Ley, 2017; J. VERVAELE, *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*, en *La Ley*, 2012, pp. 27-86; M.A. ENCINAR DEL POZO-M.A. VILLEGAS GARCÍA, *Validez de medios de prueba tecnológicos*, en *Diario la Ley*, n. 9005, 2017.

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 art. 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 comunica-*

[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 arts. 192-*bis* y 497-*bis* CP; art. 192-*bis* y art. 497-*bis*, relativos a la colocación ilegal de escuchas telefónicas, introducidos por LO 7/84 EDL1984/9281. En el ámbito procesal penal, sin embargo, no se acometió la reforma del obsoleto art. 579 LECrim, hasta la LO 4/1988 de 25 mayo 1988. Cfr. G. GALLEGO SANCHEZ, *Sobre el secreto de las comunicaciones, el art. 579 LECrim y las intervenciones telefónicas*, en *www.elderecho.com/tribuna/penal/secreto-comunicaciones-LECrim-intervenciones-telefonicas_11_159055012.html*, consulta el 16 febrero 2018, 20.07. Sobre la prueba ilícita, en esta tesitura, T. ARMENTA DEU, *Limitación de derechos fundamentales y prueba ilícita*, cit., pp. 235-237.

ciones. 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 art. 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 art 579 LECrim sólo 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 art. 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 supuestos 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 citada resoluciones del TEJUE (casos Digital Rights y Tele2 Sverige)[10], pusieron de relieve que la regulación

[7] A. E. GUDIN RODRIGUEZ-MAGARIÑOS, *La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información*, en *La Ley Penal*, n. 125, 2017.

[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).

europea sobrepasaba los límites que exige el respeto al principio de proporcionalidad requeridos por los art. 7, 8 y 52.1 de la CEDH de la Unión Europea, lo que condujo a declarar invalida la Directiva 2006/24/CE[11]. Esta anulación ha conducido a que determinados autores sostengan la STJUE de 21 de diciembre de 2016, obliga "de facto" a entender derogada la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[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 L.O. 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

[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] J.L. RODRIGUEZ LAINZ, *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*, en La Ley, n. 8308, 2014, p. 4, 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, *Encuesta Jurídica. Febrero de 2017*, Sepin (Referencia SP/DOCT/22410). A juicio de M.J. DOLZ LAGO, la sentencia afecta a la conversión de los datos (Ley 25/2007) pero no a su cesión, cfr. *op. loc. cit.*

[13] A juicio de Rodriguez Lainz y Colomer Hernandez, 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, *op. loc. cit.*

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 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 interceptación encaminadas a captar el contenido de la comunicación intervenida junto a 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 sólo 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.

[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 T. ARMENTA DEU, *Lecciones de derecho procesal*, 10ª edición, Marcial Pons, Madrid, 2017, pp. 72-74; 183-185 y 195-200.

[15] N. CABEZUDO RODRIGUEZ, *Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento en la Ley de Enjuiciamiento Criminal*, en *BMJ*, 2016, número 2186.

[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); y 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. M. MARCHENA GOMEZ, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas, Castillo de Luna, 2015, p. 201.

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 individualizadamente, 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, video) y de los datos de tráfico (fecha, hora, duración, origen y destino) una definición adecuada es la contenida en el art. 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 mail tenga lugar con ante-

[17] Se sigue la opción de J. DELGADO MARTIN, *Investigación tecnológica*, cit., capítulo 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 éste 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 art. 588-*ter* j LECrim, cuando sean datos conservados por la operadora que no sean en cumplimiento de la ley citada anteriormente; del art. 11.2 d) LO Protección de Datos, cuando sean datos conservados por la compañía a iniciativa propia; o el caso contemplado en el art. 588-*ter* LECrim.

rioridad a iniciar el proceso de comunicación o no sea así, y 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 art. 230.1 LOPJ, Ley 59/2003, art. 3 de la Firma Electróni-

[20] Si el mensaje se redacta y no sale del dispositivo afecta sólo a la intimidad, pero desde el momento 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] Arts 588-*bis* a) a art. 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. J. RUBIO ALAMILLO, *El correo electrónico como prueba en procedimientos judiciales*, en *Diario la Ley*, n. 8808, Sección Práctica Forense 21 de julio de 2016. STS 298/2015, de 13 mayo.

[23] S. PEREIRA PUIGVERT, *La exhibición de documentos y soportes informáticos en el proceso civil*, Thomson Reuters-Aranzadi, 2013, F. BUENO DE MATA, *Diligencias de investigación tecnológicas*, cit., p. 248 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. E. MARTINEZ CARVAJAL HEDRICH, *Valor probatorio de un correo electrónico*, en *diario La Ley*, n.8014, febrero 2013.

[25] Reglamento (UE), n. 910/2014, del Parlamento Europeo.

ca, y art. 299.2 LEC, por analogía, conforme a lo dispuesto en el art. 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 art. 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 sólo[29].

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 video, compartir contactos o la propia ubicación; presenta algunas diferencias con el mail y SMS, ya que la información transmitida no se conserva por un servidor externo, que se utilizan protocolos de seguridad para garantizar el cifrado de la información[30], y que

[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. J. DELGADO MARTIN, *Investigación tecnológica y prueba digital*, cit., capítulo I, p. 14 y S. PEREIRA PUIGVERT, *La exhibición de documentos*, cit.

[28] Sobre la relevancia de la pericia en éste ámbito, J.L. RODRÍGUEZ LAINZ, *Sobre el valor probatorio*, 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 ésta 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 F. DE BUENO MATA, *La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica*, en *Diario la Ley*, n. 8728, 23 de marzo, 2016.

[30] J.L. RODRÍGUEZ LAINZ, *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)*,

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

en *Diario la Ley*, n. 8569, sección doctrina, 25 de junio de 2015, ref.D-256. P. ARRABAL PLATERO, *El* WhatsApp *como fuente de prueba*, en O. FUENTES (coord.), *El proceso penal: cuestiones fundamentales*, Tirant lo Blanch, Valencia, 2017.

[31] D. GARCÍA MESCUA, *Aportación de mensajes de* WhatsApp *a los procesos judiciales. Tratamiento procesal*, Comares, Granada, 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 J.L. Rodriguez Lainz que se acaba de citar y en F. DE BUENO MATA, *La validez*, 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 figura en las tarjetas de memoria SD. J. DELGADO MARTIN, *Investigación tecnológica*, cit., capítulo 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.

resto – aportación mediante soporte 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 valorados como aceptación tácita de su autenticidad y validez;

– cuando se impugne la autenticidad, corresponde a quien lo ha aportado reforzar aquélla, 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 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].

[38] STS 300/2015, de 19 mayo; 298/2015, 13 mayo; y 786/2015, 4 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. J.L. RODRIGUEZ LAINZ, *Intervención judicial en los datos de tráfico de telecomunicaciones electrónicas*, ed. Bosch, Vallirana, 2003, pp. 391-396.

[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. T. ARMENTA DEU, *La prueba ilícita. Un estudio comparado*, 2ª ed., Marcial Pons, Madrid, 2011, pp. 141-143.

[41] Sentencia 702/2015, de 24 de noviembre, de la Sección 27ª 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 incontes-

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

table 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.*). L. DAVARA FERNÁNDEZ DE MARCOS, *Implicaciones Socio-Jurídicas de las Redes Sociales*, Thomson Reuters Aranzadi, 2015, *passim*.

[45] A. AGUSTINOY GUILAYN-J. MONCLÚS RUIZ, *Aspectos legales de las redes sociales*, cit.

[46] Se sigue en esta exposición el orden de J. DELGADO MARTIN, *Investigación tecnológica*, cit., capítulo 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: J. RODRIGUEZ LÁINZ, *Sobre el valor probatorio*, cit.

[48] La única excepción, y con el carácter específico que le otorga su ámbito de aplicación, es el art 11 b) Ley 4/2015 de 27 de abril, del Estatuto de la Víctima del delito.

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 art. 18.3 CE. Otro medio de aportación es a través de la información almacenada en un servidor, aspecto éste 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 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 Estos 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°) que las distintas informaciones insertas en el perfil abierto son colgadas libremente por lo que difícilmente afectarán al derecho a la intimidad; y 2°) 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 arts. 588 bis LECrim (con carácter general) y lo dispuesto en el art. 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 pro-

[49] Art. 276 LOPJ.

[50] Convenio sobre Ciberdelincuencia, Budapest 23 de noviembre de 2001, ratificado por España en 2010 (BOE 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 art. 10, a excepción de la 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, M. SÁEZ-SANTURTÚN PRIETO, *La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 de mayo de 2015*, en *Diario la Ley*, 2015, n. 8637 y E. MARTINEZ CARVAJAL HEDRICH, *Valor probatorio de un correo electrónico*, cit.

batoria – 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 cuestionaba, en definitiva, si tras la reforma mediante Ley Orgánica 13/2015, el umbral normativo de "gravedad" que figuraba en el art. 588-*ter* j LECrim[56] en relación con el art. 588-*ter* j LECrim[57], a la hora de adoptar la medida que permite in-

[53] Sobre el momento de apreciación: STS 255/2017, de 6 marzo y 85/2017, de 15 febrero.

[54] Nota 40, y en particular, M. SÁEZ-SATURTUN, PRIETO, *La prueba obtenida a través de mensajes en redes sociales*, cit.

[55] Accesible en *http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62016CN0207&from=ES*.

[56] Artículo 588-*ter* j. Datos obrantes en archivos automatizados de los prestadores de servicios: «Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión».

[57] Artículo 579. De la correspondencia escrita o telegráfica: «El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos: 1) Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; 2) Delitos cometidos en el seno de un grupo u organización criminal; 3) Delitos de terrorismo».

corporar al proceso los datos electrónicos de tráfico o asociados obrantes en archivos automatizados de los prestadores de servicios, salvaba el criterio de proporcionalidad, al permitir que se solicite dicha medida atendiendo únicamente a la pena que pueda imponerse por el delito que se investiga, sin requerirse identificar en la conducta delictiva un particular nivel de lesividad para bienes jurídicos individuales o colectivos. Y unido a ello, si se salvaguardan los estándares europeos utilizados por el TJUE (sentencia de 8 de abril de 2014) la determinación de la gravedad del delito atendiendo tan sólo a la pena imponible, y en tal caso, ¿Cuál sería el umbral mínimo?, y ¿lo sería una pena de tres años).

Muy resumidamente, se trataba de un caso en el que: el Sr. H. S había presentado denuncia por robo con violencia durante el cual resultó herido y le sustrajeron la cartera y el móvil. La policía solicitó al juez instructor que se ordenase a diversos proveedores de comunicaciones electrónicas la transmisión de los números de teléfonos activados en un periodo concreto, con el código relativo a la identidad internacional del equipo móvil (código IMEI) del teléfono móvil sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y en su caso, dirección. El juez denegó la diligencia por dos motivos: no ser adecuada y porque la ley limita la cesión de datos conservados por las operadoras de telefonía a los delitos graves, que son aquellos sancionados (según el CP español) los sancionados con pena de prisión superior a cinco años. Recurrido por el MP. El tribunal de apelación (Audiencia de Tarragona) plantea la cuestión prejudicial (Asunto C-207/16).

La cuestión 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 la suficiencia de la gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea; identificándolo 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 éste es compatible con una previsión general de límite de tres años de prisión, como se contempla en los arts. 579 y 588bis, ambos de la LECrim. Fuente confesada de este planteamiento es la STJUE de 8 de abril de 2014, 46 a 48, 52, y 53 y ss[58].

[58] Vid. nota 12. Adviértanse las similitudes en cuanto a discriminación de criterios tempora-

6. *La Sentencia del Tribunal de Justicia (Gran Sala), de 2 de octubre de 2018*

El tribunal asienta las cuestiones prejudiciales en si el art. 15,1 de la Directiva 2002/58 interpretada a la luz de los artículos 7 y 8 de la Carta, deben interpretarse de manera que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído (nombres, apellidos y direcciones en su caso) constituye una injerencia en los derechos fundamentales consagrados en los citados artículos, de forma que debe limitarse a la delincuencia grave. Y en tal caso, qué criterios deben determinar la gravedad del delito de que se trate.

A partir de ahí, se establecen los siguientes criterios:

a) Existe injerencia en el derecho fundamental al respeto a la vida privada por el mero acceso de las autoridades a tales datos, con independencia de que sea "grave" y sin resultar relevante que la información tenga carácter sensible o que los interesados hayan sufrido inconvenientes[59]. Al igual que constituye injerencia en el art. 8 de la Carta por ser un tratamiento de datos personales[60];

b) el art. 15, 1 Directiva 2002/58 establece con carácter exhaustivo los objetivos que pueden justificar una norma nacional que regule el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, como algo excepcional, y sin que se limite el objetivo a la lucha contra los delitos graves[61];

c) el TJUE ha declarado, que en materia de prevención, investigación, descubrimiento y persecución de delitos, sólo la lucha contra la delincuencia grave justifica el acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas. Ahora bien, ello es así, en la medida en que la injerencia en los derechos fundamentales sea proporcional a la gravedad de los delitos;

d) así las cosas, y conforme al "principio de proporcionalidad", se justifica una injerencia grave por el objetivo de luchar contra delincuencia grave; siempre y cuando, además, la injerencia también lo sea. Si la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir "delitos" en general.

---

les o falta de criterios objetivos para garantizar una limitación estrictamente necesaria, por ejemplo.

[59] Puntos 76 y 77 Informe del Abogado General.

[60] Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, EU: C: 2017: 592, apartados 124 y 126 y jurisprudencia citada.

[61] Fundamento Jurídico 52 y 53.

Como en el caso concreto, el objeto era identificar a los titulares de las tarjetas SIM activadas durante un periodo de doce días con el número IMEI del teléfono móvil sustraído, sin afectar a las comunicaciones efectuadas en el teléfono en cuestión ni la localización de éste, y a falta de un cotejo con las comunicaciones realizadas con esas tarjetas SIM y de localización, tales datos no permiten conocer la fecha, hora, duración y destinatarios de las comunicaciones efectuadas con la tarjeta SIM, ni los lugares en que las comunicaciones tuvieron lugar ni la frecuencia de estas con determinadas personas durante un periodo concreto; *no se estima injerencia grave por no permitir extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados*[62].

Y por tanto, el art. 15.1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, permite el acceso de las autoridades públicas en casos previstos en la Directiva o en la legislación nacional, siempre que no constituyan, en sí, injerencia grave en los derechos fundamentales.

7. *Las futuras órdenes europeas de entrega y conservación de pruebas penales electrónicas*

La Directiva 2014/41/CE, del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la Orden Europea de investigación en materia penal, supone un importante avance para la obtención de prueba penal transfronteriza en el ámbito de la UE[63].

Más allá, de éste importante logro, la Unión Europea se ha propuesto como una de sus prioridades esenciales para investigar y evitar determinados delitos, entre ellos los terroristas, la obtención transfronteriza de pruebas electrónicas, que pese a poderse entender incluidas en la OEI, adolece de normas específicas para alcanzar una imprescindible agilización[64]. En ésta línea surge la *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de en-*

---

[62] El subrayado es mío. Fundamento Jurídico 59 y 60.

[63] España la traspuso se realizó mediante la reforma de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, Ley 3/2018, de 11 de junio.

[64] I. GZALEZ CANO (dir.), *Orden Europea de Investigación y prueba transfronteriza*, Tirant lo Blanch, Valencia, 2019.

juiciamiento penal, de 17 de abril de 2018[65]. Mediante la misma se persigue regular la eventualidad de que las autoridades de los Estados miembros accedan a datos que puedan constituir fuente de prueba cuando estén almacenados fuera de su país, en otros Estados miembros o en terceros países. De ahí, que como novedad relevante, la orden europea de entrega no se dirija a la autoridad del Estado de ejecución sino directamente al proveedor de servicios establecidos o representado en otro Estado miembro, que es quien deberá cumplirlas, y de no ser así, el Estado de ejecución intervendrá adoptando las medidas necesarias para su ejecución, limitada a los datos almacenados, ya que la interceptación instantánea de telecomunicaciones no está cubierta por esta Propuesta, como sí sucede en los arts. 30 y 31 Directiva OEI para las pruebas transfronterizas en general[66]. Por otra parte, y completando ésta última, se ha presentado la *Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales*[67], en virtud de la cual, los proveedores de servicios deben designar un representante legal en la Unión para la recepción, el cumplimiento y la ejecución de las resoluciones y ordenes emitidas por las autoridades competentes a efectos de recabar pruebas para procesos penales.

Limita su ámbito de aplicación a órdenes a proveedores que ofrezcan sus servicios en la Unión y en el ámbito de investigaciones o procesos penales sobre infracciones determinadas producidas en la fase previa y durante el proceso, siempre y cuando, además, el proveedor de servicio esté establecido o representado en otro Estado miembro, es decir, en supuestos transfronterizos.

La Propuesta de Reglamento respeta la diferencia entre los datos de los abonados y los relativos al acceso, por una parte, cuyo impacto sobre los derechos fundamentales es menor, y los datos de transacciones y de contenido, sometiendo éstos últimos a presupuestos más estrictos: desde quien podrá emitir la OEE o la OEC, posibilidad que se veda para el Ministerio Fiscal cuando se trate de datos de transacciones y datos de contenidos[68]; hasta los requisitos, limitados en el caso de datos de transacciones o contenido, no sólo a los generales (necesidad y proporcionalidad) sino a determinadas infracciones contempladas en diversas Decisiones Marcos y Directivas: a) punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años; b) infracciones penales cometidas total o parcialmente por medio de un sistema de información (lucha contra el fraude y la falsificación de medios de pagos distintos al efectivo[69]; lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil[70], los ataques contra los sistemas de información[71], o los relativos a la lucha contra el terrorismo[72].

[65] COM (2018) 225 final.

[66] Una primera aproximación a esta iniciativa en: L. GOMEZ AMIGO, *Prueba penal electrónica en la Unión Europea: Las futuras Órdenes Europeas de entrega y conservación*, en I. GONZALEZ CANO (dir.), *Orden Europea de Investigación y prueba transfronteriza*, cit., pp. 157-159.

[67] De 17 de abril de 2018 (COM (2018) 226 final.

[68] Considerando 23 Propuesta Reglamento. Y Dictamen del Comité Económico y Social Europeo (DOUE C 367, de 10 de octubre de 2018, p. 88).

En cuanto al procedimiento, sobre el que no me extenderé por tratarse de un texto no definitivo, sólo mencionar que los "Comentarios preliminares del Coucil of Bars and Law Societes of Europe" se pronuncian críticamente en torno a tres grupos de cuestiones: a) La falta de garantía suficiente sobre un mecanismo suficiente que garantice la comunicación abogado-cliente; b) la ausencia de igualdad de medios entre acusación y defensa; y c) la omisión de una revisión judicial efectiva.

8. *Algunas reflexiones finales*

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 éste 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.

Las medidas tecnológicas presentan desafíos innegables, entre ellos: que funcionen, que la interoperatividad de los medios sea rea, y la seguridad. A ello se une la forma de acceso a la fuente probatoria, y el alcance del principio de proporcionalidad, y la forma y garantías del ya medio probatorio al proceso para alcanzar validez probatoria.

La incidencia de estos desafíos y otros que hayan quedado en el tintero presentan, al menos tres vertientes que sólo pueden mencionarse en esta sede:

[69] Definidos en los arts. 3 a 5 de la Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001.

[70] Arts. 3 a 7 de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo.

[71] Arts. 3 a 8 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013.

[72] Arts 3 a 12 y 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017.

a) la externalización de la justicia o de parte de ella; b) la relevancia de la prueba pericial; y la proyección de la inteligencia artificial[73].

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 sólo la garantía de ambos extremos enerva válidamente la presunción de inocencia[74]. 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)[75].

La incidencia de las pruebas tecnológicas en la prueba ilícita conecta directamente con la injerencia que la adopción de la medida de investigación tenga en los derechos fundamentales, ya se trate de los recogidos en la Carta Europea, ya los contemplados en los textos nacionales. En tal sentido, y a partir de la nueva Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, el principio de proporcionalidad actúa como parámetro para medir el alcance de dicha injerencia, que cuando alcanza un determinado grado de gravedad, como permitir o propiciar extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, tal como sucedía en el caso resuelto por la STJUE de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros) que acarreo la anulación de la Directiva 2006/24 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.*

Los atentados en diversas ciudades europeas y el innegable crecimiento de una delincuencia tecnológica han desplazado el péndulo hacia un reforzamiento de los medios de investigación y una cierta limitación en la protección de las garantías, especialmente cuando se trata de medidas que afectan a la

[73] Estos tres aspectos fueron expuestos en una conferencia de F. GASCÓN INCHAUSTI, *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, en *el Congreso VI Processulus: La justicia digital en España y la Unión Europea: Situación actual y perspectivas de futuro*, Cáceres, 16 y 17 de mayo de 2019, pendiente de publicación.

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

[75] STS 255/2017, de 6 de marzo, F.J. nº 8 y STS 675/ 2015, de 10 de noviembre y 250/2017, F.J, n. 6.

prueba electrónica y al acceso a los datos almacenados en los servidores. En esta línea la OEI y la Propuesta de Reglamento sobre órdenes europeas de entrega y conservación de pruebas electrónicas facilita la obtención y entrega de *pruebas (y pruebas electrónicas*[76]) en el marco de la UE, asumiendo, no obstante, las categorías europeas que persiguen salvaguardar un círculo de mayor protección para aquellos datos susceptibles de causar un mayor impacto en los derechos fundamentales, discriminando el régimen legal aplicable a los datos almacenados que pueden ser solicitados a través de tales órdenes, cuando se trata de datos de los abonados y los relativos al acceso, en los que la afección es menor, y los datos de transacciones y de contenidos, en los que la afectación de derechos fundamentales es mayor, de manera que los primeros.

[76] Se trata en realidad de fuentes de pruebas; de ahí el entrecomillado.