

LA (FUTURA) ORDEN EUROPEA DE ENTREGA DE PRUEBAS ELECTRÓNICAS

OLGA FUENTES SORIANO

*Universidad Miguel Hernández
Catedrática de Derecho Procesal*

SUMARIO: I. INTRODUCCIÓN; II. CONCEPTO Y ÁMBITO DE APLICACIÓN; III. LA AUTORIDAD EMISORA DE LA ORDEN; IV. EL DESTINATARIO DE LA ORDEN; V. REQUISITOS OBJETIVOS DE LA ORDEN: PROPORCIONALIDAD Y NECESIDAD; VI. BIBLIOGRAFÍA.

Resumen: La Orden de entrega de pruebas electrónicas es una iniciativa legislativa de la Unión Europea, actualmente en fase de tramitación, que pretende crear un instrumento procesal específico para facilitar y agilizar la investigación criminal entre los distintos Estados miembros, en aquellos supuestos —hoy prácticamente inevitables— en los que entra en juego información digital relevante para el esclarecimiento de la comisión delictiva.

Palabras clave: Prueba electrónica; proceso penal; reconocimiento mutuo; cooperación judicial.

I. INTRODUCCIÓN

En los últimos tiempos, propiciado por el carácter transnacional de la actuación delictiva así como por la necesidad de consolidar el Espacio de Libertad, Seguridad y Justicia sobre el que se construye la Unión Europea, asistimos a una proliferación de instrumentos procesales que buscan establecer cauces ciertos de cooperación jurídica a fin de favorecer y agilizar la tramitación de los procesos y la investigación criminal.

Entre los mecanismos institucionales comunes que en las últimas décadas han visto la luz, cabe citar, *u. gr.*, la Orden europea de detención y entrega¹, el exhorto

¹ La Orden Europea de Detención y entrega ha sido considerada el desencadenante de toda una serie de instrumentos normativos acordados con posterioridad tendentes a establecer unos mínimos comunes sobre las garantías de imputados y víctimas en el proceso penal, a nivel europeo. Sobre el establecimiento de una normativa común que regule el tratamiento, derechos y garantías de los acusados y sospechosos en el proceso penal —con cita detallada de las Directivas emitidas al efecto— puede verse LARO GONZÁLEZ, M.E., “Derechos y garantías del menor

européo para la obtención de prueba o, por fin, la Orden europea de investigación.

Es, sin duda, ésta última la que focaliza las mayores esperanzas de éxito respecto de la investigación (y prueba) de la delincuencia de carácter transnacional; pero la mencionada Orden europea de investigación no contiene referencia alguna a la práctica concreta de diligencias de investigación de carácter electrónico que se ha convertido en pieza clave de la práctica totalidad de los procesos penales.

Ante la gravedad de muchos de los hechos a que se puede tener acceso mediante información de carácter electrónico —pruebas, pues, electrónicas—, su creciente y exponencial utilización y las peculiaridades propias de éstas, que exigen —o cuanto menos, aconsejan— un tratamiento individualizado de las mismas, el legislador europeo, se enfrenta a la tesitura de, o bien reformar la Directiva de 2014 que regula la Orden europea de investigación, para darles cabida o bien, crear *ex novo* un instrumento normativo que atienda a estas específicas particularidades. Su opción, finalmente, le ha llevado a decantarse por esta última posibilidad y, en consecuencia, en el año 2018 la Comisión Europea aprobó dos importantes iniciativas legislativas tendentes a hacer frente a la siempre difícil obtención de prueba transfronteriza, especialmente significativa cuándo presentan éstas carácter digital: la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (COM (2018) 225 final, 2018/0108 (COD) y la Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales (COM (2018) 226 final, 2018/2017 (COD).

Al estudio de algunos aspectos fundamentales que delimitan la finalidad y estructura de la proyectada Orden de entrega de pruebas electrónicas en los procesos penales se dedicarán las páginas que siguen, dejando para otro momento, por razones de espacio derivadas de la participación en una obra colectiva, el estudio de la Orden de conservación de pruebas, igualmente electrónicas, reguladas en ese mismo Proyecto legislativo².

en el proceso penal. Armonización legislativa y necesidades procesales”, La Ley Unión Europea, N° 73, 30 de septiembre de 2019, Wolters Kluwer (p. 1). Destaca la autora, en todo caso, como esa necesaria armonización procesal de la que parece haberse tomado conciencia en lo que al proceso de adultos respecta, se encuentra ausente de cualquier referencia en el proceso penal de menores salvo por lo que respecta a la Directiva (UE) 2016/800 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales.

² He abordado el tema con mayor extensión en “Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las Órdenes europeas de entrega y conservación de pruebas electrónicas”, *Era Digital, Sociedad y Derecho* (Dir. FUENTES SORIANO

II. CONCEPTO Y ÁMBITO DE APLICACIÓN

El art. 2 (1) de la Propuesta de Reglamento que regula la proyectada Orden europea de entrega de datos electrónicos la concibe como aquella “decisión vinculante adoptada por una autoridad emisora de un Estado miembro que obligue a un proveedor que ofrezca servicios en la Unión y esté establecido o representado en el territorio de otro Estado miembro a entregar pruebas electrónicas”.

De la definición expuesta cabe extraer numerosos aspectos en los que conviene profundizar a fin de dejar correctamente perfilado su concepto y extensión.

En primer lugar, la Orden de entrega se concibe como una decisión vinculante de carácter unilateral, lo que supone que, efectivamente, una vez aprobado el Reglamento, cualquier Estado miembro podrá hacer uso de ella obligando así al destinatario (proveedor de servicios en otro Estado miembro) a dar cumplimiento a la misma. Se regulan, no obstante, en la propuesta de Reglamento, motivos tasados para su no cumplimiento por parte del destinatario; pero, en principio y a salvo esas excepcionales situaciones, si la Orden cumple con los requisitos legales establecidos, su emisión vincula directamente al proveedor de servicios a su cumplimiento.

En segundo lugar, la Orden de entrega de pruebas electrónicas es un instrumento procesal propio de la Unión con lo que su utilización queda restringida a los Estados miembros y, concretamente, dentro de estos, a las autoridades emisoras o autoridades a las que se reconoce capacidad de emisión de las mismas —que se analizarán en el epígrafe siguiente—. La cuestión no es en absoluto baladí porque, precisamente, el hecho de que la Orden de entrega de pruebas electrónicas sea un recurso procesal exclusivamente europeo obligará a buscar nuevas fórmulas de cooperación entre la Unión Europea y terceros Estados en lo que a la obtención de prueba transfronteriza respecta. Justamente en este contexto se enmarca la “Recomendación de Decisión del Consejo por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal”, de 5 de febrero de 2019³.

En la actualidad, la cooperación de los Estados de la Unión Europea con los EEUU de América se centra en torno a datos sin contenido. Por “datos sin conte-

O.), Tirant lo Blanch, Valencia, 2020, pp. 281 a 343. El presente trabajo constituye, pues, una exposición muy resumida de algunos aspectos esenciales allí tratados con mayor profundidad.

³ COM (2019) 70 final. Sobre los objetivos y las directrices de negociación contenidas en la Recomendación de Decisión de referencia puede verse GÓMEZ AMIGO, L., “Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima”, *Revista Española de Derecho Europeo*, n° 71, julio-septiembre 2019, pp. 23 a 56 (sobre el tema, en concreto, pp. 50 a 53).

nido” cabe entender aquellos que proporcionan información sobre, por ejemplo, los abonados o sobre el tráfico de una cuenta en línea; mientras que los “datos de contenido”, hacen referencia, *u. gr.*, a correos electrónicos, mensajes de texto, fotografías, vídeos, etc. Actualmente, las autoridades de un Estado miembro de la Unión pueden dirigir una solicitud de datos sin contenido a los proveedores de servicios instalados en EEUU y, la legislación de este país les permite colaborar, siempre de forma voluntaria, entregando esos datos solicitados. Esta posible actuación voluntaria genera cierto margen de inseguridad jurídica para los Estados europeos solicitantes y “además, —en palabras de la Exposición de Motivos de la Recomendación de Decisión— puede resultar poco fiable, es posible que no respete las garantías procesales pertinentes, solo es viable con un número limitado de proveedores de servicios que aplican todas políticas distintas, no es transparente, y carece de un mecanismo de rendición de cuentas. La fragmentación resultante puede generar inseguridad jurídica, dudas sobre la legalidad del proceso y preocupaciones en torno a la protección de los derechos fundamentales y las garantías procesales de las personas relacionadas con tales solicitudes”⁴. La necesidad, pues, de establecer cauces de comunicación y actuación que favorezcan la obtención de pruebas electrónicas entre Europa y EEUU —y que complementen, en el ámbito correspondiente, a los mecanismos de obtención de prueba transfronteriza europeos— resulta palmaria, especialmente si se tiene en cuenta que es precisamente allí donde tienen su sede los mayores proveedores de servicios mundiales.

En tercer lugar, de la definición anteriormente anotada se desprende, con absoluta claridad, que la Orden de entrega europea ha de ser remitida por —y desde— un Estado miembro a un proveedor de servicios que se encuentre en otro Estado miembro distinto. Es decir, que la Orden de entrega de pruebas electrónicas ha de serlo, exclusivamente, para pruebas de carácter transfronterizo, en este sentido entendidas.

Y, en cuarto y último lugar, la Orden de entrega europea de entrega rige, exclusivamente, para lo que genéricamente conocemos como pruebas electrónicas; entendiéndose por tales aquellas que ofrecen información sobre datos almacenados, difundidos o tratados electrónicamente, sean estos con contenido o sin contenido⁵.

⁴ Explanatory memorandum. Recommendation for a COUNCIL DECISION authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters COM/2019/70 final. 1. Context.

⁵ Han sido muchos los calificativos añadidos al concepto de prueba para denotar la idea de una información extraída a partir de datos informáticos: esto es, datos obtenidos, almacenados, difundidos...mediante procedimientos informáticos y, por tanto, electrónicos. Se ha hablado así de prueba electrónica, telemática, digital, cibernética, tecnológica, prueba del hecho digital, etc.

En definición de la propia Propuesta de Reglamento —art. 2 (6)—⁶, por “pruebas electrónicas” a efectos de las órdenes europeas de entrega y conservación cabría entender “pruebas almacenadas en formato electrónico por un proveedor de servicios o en nombre del mismo en el momento de la recepción de un certificado de Orden europea de entrega o de un certificado de Orden europea de conservación, consistentes en datos de los abonados, datos relativos al acceso, datos de transacciones y datos de contenido almacenados”⁷.

El hecho de tratarse, en todo caso, de información relativa a datos personales hace especialmente atendibles todas las exigencias que requiere el debido respeto a los derechos fundamentales⁸, más allá del necesario cumplimiento del conjunto de la normativa comunitaria sobre protección de los mismos⁹.

De todos ellos, el de prueba tecnológica ha sido el más utilizado en las últimas reformas procesales; sin embargo, resulta éste perfectamente intercambiable con el de prueba electrónica que esta Propuesta de Reglamento Europeo. Sobre el tema, *in extenso*, vid. ARRABAL PLATERO, P., *La prueba tecnológica. Aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019, pp. 29 a 39, para quien “la prueba tecnológica hace referencia, por un lado, a aquellos datos informáticos, esto es, los impulsos electrónicos susceptibles de ser «almacenados en cualquier parte del planeta, enviarse al otro extremo del globo en cuestión de segundos, ser alterados o clonados rápidamente, guardarse en carpetas ocultas, servidores lejanos, cifrados, etc.» con trascendencia en un proceso —véase un pen drive o un disco duro— y, por otro, a aquellos elementos obtenidos a través de medios tecnológicos —como, por ejemplo, un peritaje informático, comunicaciones interceptadas por medio de mecanismos tecnológicos, ...— (Op. cit., p. 33)

⁶ Llama la atención, en este punto, que mientras en la propuesta de Reglamento en Inglés la definición de pruebas electrónicas del art. 2 consta en el número 6; en el documento elaborado en Castellano por la comisión, dicha propuesta ocupa el número 5 de ese mismo precepto legal.

⁷ En los supuestos en los que los datos —la prueba— se almacena por un tercero en nombre de un proveedor de servicios determinado, será este tercero quien ostentará la condición de encargado del tratamiento de los datos del prestador de servicios. En este sentido MONTORO SÁNCHEZ, J.A., “Breve análisis acerca del futuro Reglamento Comunitario “E-Evidence” sobre las órdenes europeas de conservación y entrega de pruebas y evidencias electrónicas a efectos de enjuiciamiento penal”, en *Orden europea de investigación y prueba transfronteriza en la unión europea*, GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019, p. 176.

⁸ Sobre la construcción y alcance del derecho a la protección de datos como derecho fundamental puede verse ARRABAL PLATERO, P., “La videovigilancia laboral cómo prueba en el proceso”, *Revista General de Derecho procesal*. Iustel, n° 37, 2015, pp. 11 y ss. Sobre las exigencias de especialidad, idoneidad, excepcionalidad y necesidad de la medida y, por último, proporcionalidad como requisitos de su limitación, he tenido ocasión de pronunciarme en “Comunicaciones telemáticas: práctica y valoración de la prueba”, en *El proceso penal. Cuestiones fundamentales* (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017. Al respecto también BUENO DE MATA, F., *Las diligencias de investigación penal (...)*, cit., pp. 30 a 38; sobre la obligación de colaboración de los servidores situados fuera de España, pp. 71 a 76.

⁹ Así se manifiesta en el Considerando 2 de la propuesta de Reglamento “Unos mecanismos eficaces para obtener pruebas electrónicas [en referencia a las Órdenes europeas de entrega y conservación] son esenciales para combatir la delincuencia, siempre que se respeten unas con-

Es de resaltar, por último, aunque no derive de la definición de Orden europea de entrega de pruebas electrónicas que ofrece el art. 2 de la Propuesta de Reglamento que se analiza, que esta Orden podrá utilizarse tan sólo en el seno de un proceso penal ya iniciado. Es decir, que aquellas pruebas electrónicas transfronterizas que pudieran resultar relevantes para la tramitación de un proceso civil, laboral o contencioso-administrativo no podrán solicitarse directamente por el Estado interesado al proveedor de servicios establecido en otro Estado mediante la remisión de este instrumento legal.

Asentado así el ámbito penal como el propio en el que podrá desenvolverse la Orden que nos ocupa, se centrará la atención, a partir de este momento, en profundizar en otros aspectos importantes que contribuyen, a la delimitación de su ámbito de aplicación.

En primer lugar, cabría recordar que el hecho de que la Orden europea de entrega de pruebas electrónicas lo sea respecto de aquéllas que presentan carácter transfronterizo supone que dicha Orden será tan sólo aplicable —tan sólo dirijible— frente a proveedores de servicios que los presten en Estados distintos de aquél que emite la Orden. Nunca podrá utilizarse, pues, en entornos nacionales por mucho que se pretenda con ella recabar datos sobre sujetos o comunicaciones extrafronterizos. El carácter transnacional de la prueba viene marcado por el lugar de establecimiento o vinculación del prestador de servicios destinatario de la Orden que es, en suma, quien ha de cumplirla y entregar los datos requeridos. La distinta ubicación del proveedor de servicios respecto del Estado emisor de la

diciones que garanticen la plena conformidad con los derechos fundamentales y los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea y consagrados en los Tratados, en particular, los principios de necesidad y proporcionalidad, las garantías procesales, la protección de datos, la confidencialidad de la correspondencia y la intimidad”. Esta insistencia en el necesario respeto al acervo comunitario sobre protección de datos se concreta claramente en el detalle de las precauciones que los distintos sujetos implicados por una orden de entrega han de tomar en consideración; así, el Considerando 57 establece que “los datos personales obtenidos en virtud del presente Reglamento deberán tratarse solo cuando sea necesario y ser proporcionados para fines de prevención, investigación, detección y enjuiciamiento de delitos, la aplicación de sanciones penales y el ejercicio de los derechos de la defensa. En particular, los Estados miembros deberán garantizar que se apliquen las políticas y medidas pertinentes en materia de protección de datos a la transmisión de datos personales de las autoridades competentes a los proveedores de servicios para los fines del presente Reglamento, así como las medidas destinadas a garantizar la seguridad de los datos. Los proveedores de servicios deberán garantizar lo mismo para la transmisión de datos personales a las autoridades pertinentes. Solo personas autorizadas deberán tener acceso a información que contenga datos de carácter personal que puedan conseguirse a través de procesos de autenticación. Deberá considerarse la utilización de mecanismos que garanticen la autenticación, como los sistemas nacionales de identificación electrónica notificados o los servicios de confianza con arreglo a lo dispuesto por el Reglamento (UE) n.º 910/2014 del Parlamento Europeo”.

Orden es lo que marca el carácter transnacional o transfronterizo de la prueba que se pretende obtener.

Si bien sobre el carácter de los proveedores de servicios se profundizará en el epígrafe siguiente, al tratar los requisitos subjetivos de la emisión de una Orden europea de entrega, conviene referir ahora, para delimitar el ámbito de aplicación de la Orden, los distintos tipos de datos que a través de ésta se pueden recabar.

La Propuesta de Reglamento reconoce cuatro tipos de datos para cuyos procedimientos de entrega establecerá relevantes matices diferenciales por cuanto la afeción de derechos fundamentales variará, notablemente, en función de aquéllos a los que se refiera la Orden. Se diferencian así, en la Propuesta: 1) los datos de los abonados; 2) los datos relativos al acceso; 3) los datos de transacción; y, por último 4) los datos de contenido.

A la vista de las definiciones del art. 2 de la Propuesta de Reglamento, por “datos de los abonados” cabrá entender cualquier dato en relación con la identidad del abonado o cliente (como nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, teléfono o dirección de correo electrónico); así como cualquier dato en relación con el tipo de servicio y su duración, incluyendo aquí los datos técnicos que identifiquen las medidas técnicas correspondientes o las interfaces, utilizadas o facilitadas al abonado o cliente, y los datos relativos a la validación del uso del servicio, excluyendo las contraseñas u otros medios de autenticación utilizados en lugar de una contraseña que hayan sido facilitados por el usuario o creados a petición del usuario.

Los “datos relativos al acceso” son aquéllos que versan sobre el inicio y final de una sesión de acceso del usuario a un servicio, y que sean estrictamente necesarios para identificar al usuario del servicio (*v. gr.* la fecha y hora del acceso, o de conexión y desconexión al servicio, junto con la dirección IP asignada al usuario por el proveedor de servicios de acceso a internet, los datos identificativos de la interfaz utilizada y la identificación del usuario). Se incluyen, en este ámbito también, los metadatos de comunicaciones electrónicas¹⁰. La referencia expresa a este tipo de datos —los datos relativos al acceso— llama la atención por cuanto se recogen *ex novo* en la Propuesta, separándose así este instrumento legislativo

¹⁰ Según el art. 4, apartado 3, letra C) —que no g, como sostiene la propuesta de Reglamento— de la Propuesta de Reglamento relativo al respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas por “metadatos de comunicaciones electrónicas” cabrá entender cualesquiera “datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; se incluyen los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación”

de las referencias habituales en la normativa de los diversos Estados europeos que reconocen, normalmente, la existencia de, tan sólo, los datos de los abonados, los de transacciones y los de contenido. En todo caso y como se verá a continuación, los datos relativos al acceso presentan características comunes con los datos de los abonados y ello permitirá, en muchas ocasiones, darles un tratamiento procesal conjunto.

Los “datos de transacciones” hacen referencia —como su nombre indica y siempre según el concepto que el art. 2 de la Propuesta de Reglamento facilita— a datos *sobre transacciones relacionadas con la prestación de un servicio ofrecido por el proveedor, que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del propio proveedor de servicios, tales como el origen y destino de un mensaje u otro tipo de interacción, la ubicación del dispositivo, la fecha, la hora, la duración, el tamaño, la ruta, el formato, el protocolo utilizado y el tipo de compresión, a menos que estos datos constituyan datos relativos al acceso*. Igual que se ha previsto respecto de los datos de acceso, también se incluyen aquí los metadatos de las comunicaciones electrónicas, según se definen en la Propuesta de Reglamento relativo al respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas, anteriormente referida. Sin embargo, a diferencia de los datos de acceso (y de los abonados) que no proporcionan información alguna sobre los sujetos que intercomunican con el usuario, los datos de transacciones, permiten obtener información sobre los contactos y el paradero del usuario, y pueden servir para establecer el perfil de un individuo.

Los enumerados hasta aquí constituyen lo que se ha dado en denominar “datos sin contenido” y respecto de los cuales, voluntariamente, los proveedores de servicios pueden hacer entrega a las autoridades judiciales o policiales siempre con respeto a las exigencias legales derivadas de la necesaria protección de datos.

Frente a estos datos sin contenido se alzan, por último los denominados “datos de contenido” y que se refieren a cualquier dato almacenado en formato digital, como texto, voz, vídeos, imágenes y sonidos, distintos de los datos de los abonados, los datos relativos al acceso o los datos de transacciones.

Si bien se observa y según se ha adelantado, los dos primeros tipos de datos analizados (datos de los abonados y datos relativos al acceso) tienden a un mismo objetivo; al objetivo común y básico de identificar al usuario. En este sentido difieren notablemente de los otros dos grupos de datos (los de transacciones y los de contenidos) cuyo objetivo es añadir alguna información adicional a esa identificación inicial. Habida cuenta la diferencia informativa que proporcionan unos y otros, es cierto que la injerencia que producen en los derechos fundamentales y, con ello, las salvaguardias y exigencias a tener en cuenta, serán muy distantes

en uno u otro caso¹¹. Y ello siempre desde la consideración de que, en tanto en cuanto afectan —en mayor o menor medida— al derecho a la protección de datos, les será de aplicación todo el acervo normativo comunitario destinado a dicha protección.

La obtención, entrega y tratamiento de los datos de los abonados y los de acceso está sometida a requisitos menos estrictos que los que se aplican a los de transacciones y de contenido, sin duda, en estos últimos supuestos, por su mayor sensibilidad. En ese sentido, mientras que para la emisión o validación de una Orden europea de entrega de datos de los abonados o de acceso está previsto aceptar como suficiente la intervención del fiscal competente, para obtener datos de transacciones y de contenido se requerirá siempre de la intervención de la autoridad judicial.

Paralelamente y por los mismos motivos, mientras que la Orden europea de entrega de datos de los abonados o de los relativos al acceso puede emitirse ante la comisión de cualquier tipo de infracción penal, la Orden de entrega de datos de transacciones o de contenido va a quedar limitada a un ámbito objetivo mucho más restringido.

Así, la Propuesta de Reglamento ha buscado fórmulas de limitación del ámbito objetivo de las órdenes de entrega de pruebas electrónicas cuando se refieren a datos sobre transacciones o de contenido; y de entre la clásica opción de atender a un criterio de limitación penológico cuantitativo o a una selección de supuestos de carácter cualitativo (esto es, en atención al *quantum* de la pena o a las conductas sancionables) opta, en suma, por una combinación de ambos criterios.

Establece así, por una parte —art. 5 4 (a) —, que sólo será viable una Orden de entrega de pruebas electrónicas que afecte a datos de transacciones o de contenido cuando se emita *frente a delitos cuyo límite máximo de pena no sea inferior a tres años*.

Y, junto con ello, por otra parte —art. 5 4 (b)—, se admite la válida emisión de estas Órdenes de entrega de datos cuando se trate de la investigación y enjuiciamiento de las conductas delictivas que determina específicamente, con independencia de la pena con que se encuentren sancionadas, siempre que hayan sido cometidas a través de un sistema de información¹². Concretamente, se trata, de la

¹¹ Claramente lo expresa el Considerando 23 de la Propuesta al reconocer que “mientras que los datos de los abonados y los datos relativos al acceso son útiles para obtener unos primeros indicios en una investigación sobre la identidad de un sospechoso, los datos de transacciones y los datos de contenido son más relevantes como material probatorio”.

¹² Según definición de la *Directiva 2013/40/UE* del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, DO L 218 de 14.8.2013, p. 8), por “sistema de información” cabe entender “todo aparato o grupo de aparatos interconectados o

comisión de determinados delitos en relación con el fraude y falsificación de medios de pago, delitos sexuales sobre menores, delitos cometidos contra sistemas de información y delitos de terrorismo¹³.

III. LA AUTORIDAD EMISORA DE LA ORDEN

La referencia legal a la autoridad emisora¹⁴ (y no al Estado emisor) supone determinar, como punto de partida, qué institución o instituciones están en condiciones de emitir una Orden de entrega de pruebas electrónicas. Y llegados a este punto, la dispar regulación de los Estados miembros —los distintos sistemas procesales vigentes en la Unión—¹⁵ obligará a formular las normas con una laxa y premeditada vocación de generalidad desde la que poder dar cobertura a esa diversa realidad procesal.

Así, y a partir de la distinción anteriormente mencionada entre las menores exigencias requeridas para la obtención de datos de los abonados y de acceso, por un lado y los mayores requerimientos exigidos para los datos de transacciones y de contenido por otro, diferencia la Propuesta de Reglamento entre las autoridades a las que reconoce competencia para emitir la Orden en uno u otro caso¹⁶.

Cuando de datos relativos al acceso o a los abonados se trata, la emisión de la Orden de entrega resultará notablemente menos formalista y podrá provenir de una diversidad de autoridades que, sin embargo, no se contemplan cuando del resto de datos se trate. Así, podrá ser emitida —en el primer caso— no sólo por cualquier autoridad judicial o fiscal sino, también, por cualquier otra autoridad

relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento” (art. 2, a)

¹³ Los conductas delictivas concretas relacionadas en el precepto son (art. 5.4.b): *las definidas en los artículos 3, 4 y 5 de la Decisión marco 2001/413/JAI del Consejo; las definidas en los artículos 3 a 7 de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo; las definidas en los artículos 3 a 8 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo; y en la letra c) las infracciones penales definidas en los artículos 3 a 12 y 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo*

¹⁴ Vid. art. 4 de la Propuesta de Reglamento para su definición.

¹⁵ Sobre la necesidad de establecer un sustrato normativo probatorio común para los distintos países de la UE puede verse ORMAZÁBAL SÁNCHEZ, G., “El tortuoso camino hacia la construcción del espacio judicial europeo en materia penal. Algunas consideraciones en torno al reconocimiento mutuo de pruebas, la euroorden y la Fiscalía Europea” en *Derecho y proceso. Liber Amicorum del Profesor Francisco Ramos Méndez* (CACHÓN CADENAS y FRANCO ARIAS, Coords.), Barcelona 2018, pp. 1805 y ss

¹⁶ Cfr. Art. 4 apartados 1 y 2.

a la que en el Estado se le haya reconocido competencia en materia de investigación penal siempre que, en éste último supuesto, la Orden sea validada previo examen del cumplimiento de las condiciones de emisión por un juez o fiscal del propio Estado emisor. La intervención, pues de Juez o fiscal, bien para la emisión, bien para la validación de una Orden de entrega que afecte a datos de acceso o relativos a los abonados, resultará necesaria en todo caso; pero nótese que puede la intervención —la emisión o la validación de la Orden— provenir del Juez, o también del Fiscal.

Frente a ello, sin embargo, habida cuenta su mayor afección a los derechos fundamentales en juego, la Orden de entrega que se refiera a datos de transacciones o de contenido habrá de ser emitida por una autoridad judicial, admitiéndose tan sólo la proveniente de otra autoridad a la que en el Estado se le hayan reconocido competencias para la investigación penal cuándo haya sido validada, necesariamente, por una autoridad judicial¹⁷. Sin duda, estamos ante una clara manifestación expresa de la jurisdiccionalidad que se exige como requisito para la limitación de derechos fundamentales.

A la vista de la anterior propuesta de regulación cabría tomar en consideración dos puntos de vista planteados para su mejora. Por un lado, que la ausencia de una regulación expresa que permita a los acusados solicitar una Orden de entrega en las mismas condiciones que se reconoce al Ministerio Fiscal ha sido vista por la Abogacía Europea como un claro ataque al principio de la igualdad de medios entre la acusación y la defensa, que coloca al acusado en una situación de desventaja¹⁸. Y por otro lado, que la posibilidad de que el Ministerio Fiscal pueda emitir estas Órdenes, aun cuando estén referidas a datos de acceso o de los abonados ha sido vista por el Comité Económico y Social Europeo, como atentatoria contra la normativa europea de protección de datos, plantándose así la conveniencia de que, en todo caso, la emisión de las mismas tenga que provenir de una autoridad judicial¹⁹.

¹⁷ Cabe tener presente que la autoridad que valida la orden en los supuestos analizados pasa a ser considerada como autoridad de emisión a efectos de transmitir el Certificado EPOC y EPOC-CR contemplado en los anexos de la normativa, que constituye el cauce formal de transmisión de las Órdenes de referencia. Art. 4.4 de la Propuesta de Reglamento.

¹⁸ Cfr. https://www.cbbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf (p. 6)

¹⁹ *Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal [COM(2018) 225 final-2018/0108 (COD)]- 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*

IV. EL DESTINATARIO DE LA ORDEN

El destinatario de la proyectada Orden de entrega de pruebas electrónicas será —con los matices que se verán a continuación— el proveedor de servicios del que se requieren los datos solicitados.

Aquí radica, precisamente, una de las novedades importantes de esta regulación. El hecho de que la solicitud de entrega se dirija directamente frente a quien tiene los datos que se solicitan (sin necesidad de recurrir a ninguna autoridad interpuesta que ejerciera de intermediaria en su tramitación) y el reconocimiento de su carácter vinculante y, por tanto, de obligado cumplimiento para el proveedor de servicios agilizará sin duda esa obtención, teniendo en cuenta además, los tasados motivos de incumplimiento —de no ejecución— de la Orden y los breves plazos de respuesta concedidos.

Pero esta mayor agilidad en la obtención de la prueba puede chocar contra determinados derechos fundamentales del investigado, como el derecho de defensa, por no resultar necesaria la supervisión de la Orden por las autoridades del Estado receptor de la misma, así como por el hecho de que el investigado no pueda realizar alegaciones previas ni en el Estado emisor ni en el de recepción de la Orden²⁰. Es, una vez más, el reflejo de la eterna tensión entre la mayor agilidad en los procedimientos y la necesidad de hacerlo salvaguardando los derechos fundamentales en juego. Pero efectivamente, el sistema propuesto por el Reglamento convierte el control jurisdiccional sobre la obtención de una prueba que afecta de lleno a los derechos fundamentales en un control meramente eventual, que tendrá lugar tan sólo cuando el proveedor de servicios —entidad privada— se niegue a la ejecución de la Orden. Se ha sostenido que de prosperar, esta propuesta supondría la “privatización” del reconocimiento mutuo²¹.

En este contexto, una de las principales preocupaciones de la normativa es la de delimitar con precisión quiénes tendrán, a estos efectos, la consideración de proveedores de servicios; y, de conformidad con lo establecido en el art. 2 (3)²²,

procesos penales [COM(2018) 226 final-2018/0107(COD)]. 2018/C 367/17. En su Conclusión 1.7. puede leerse que “el CESE acoge con satisfacción que ambas Órdenes deban ser emitidas o confirmadas por una autoridad judicial de un Estado miembro. Sin embargo, el CESE considera problemático que, para la obtención de datos de los abonados y de datos relativos al acceso, los fiscales también puedan emitir Órdenes de entrega y respalda que la obtención de los datos de carácter personal se someta a la autorización de un juez”.

²⁰ En este sentido MONTORO SÁNCHEZ, J.A., “Breve análisis (...), *cit.*”, p. 183

²¹ Cfr. GÓMEZ AMIGO, L., “Las Órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima”, *Revista Española de Derecho Europeo*, n° 71, julio-septiembre 2019, pp. 23 a 56 (en concreto, p. 54).

²² Nótese que en el texto en Castellano de la Propuesta de Reglamento, esta referencia se encuentra en el art. 2 (2) y no así 2 (3) como consta en el texto de la propuesta en Inglés.

se considerarán proveedores de servicios quienes, con independencia de que sean personas físicas o jurídicas y tengan o no establecimiento en el Estado de la Unión en el que se les requiere, presten uno o varios de los servicios que el precepto especifica y que se refieren a: A) Servicios de comunicaciones electrónicas²³; B) servicios de la sociedad de la información²⁴, que cuenten con el almacenamiento de datos como componente esencial del servicio prestado al usuario, en particular las redes sociales, los mercados en línea que faciliten transacciones entre sus usuarios, y otros servicios de alojamiento de datos; y C) servicios de asignación de nombres de dominio de internet y de direcciones IP, tales como proveedores de direcciones IP y registradores de nombres de dominio, así como servicios de privacidad y representación relacionados.

Para la remisión a estos proveedores de servicios de una Orden de entrega, se ha sostenido que no es necesario que tengan establecimiento fijo en el Estado de la Unión en el que son requeridos; lo que la normativa exige es que entre el proveedor de servicios y el Estado en el que los presta se de tan sólo una “estrecha vinculación”. Y si bien es cierto que el mejor exponente de dicha estrecha vinculación podría venir constituido por la existencia de un establecimiento del proveedor de servicios en el Estado²⁵, se admite también la valoración de otros

²³ Por servicio de comunicación electrónica, según se define en el artículo 2, apartado 4, de la Directiva por la que se establece el Código Europeo de Comunicaciones Electrónicas, cabe entender aquél prestado “por lo general a cambio de una remuneración a través de redes de comunicaciones electrónicas, que incluye, con la excepción de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos, los siguientes tipos de servicios: a) el «servicio de acceso a internet», entendido según la definición del punto 2) del párrafo segundo del artículo 2 del Reglamento (UE) 2015/2120; b) el «servicio de comunicaciones interpersonales», y c) servicios consistentes, en su totalidad o principalmente, en el transporte de señales, como son los servicios de transmisión utilizados para la prestación de servicios máquina a máquina y para la radiodifusión”

²⁴ Por servicios de la sociedad de información, según se definen en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, cabe entender “todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios”. Y a efectos de matizar el tenor del precepto, se establece a renglón seguido que “se entenderá por: i) «a distancia», un servicio prestado sin que las partes estén presentes simultáneamente, ii) «por vía electrónica», un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, iii) «a petición individual de un destinatario de servicios», un servicio prestado mediante transmisión de datos a petición individual”.

²⁵ Por “establecimiento” entiende la Propuesta de Reglamento el “*ejercicio efectivo de una actividad económica por tiempo indefinido a través de una infraestructura estable a partir de la cual*

indicadores como el hecho de contar con un significativo número de usuarios, la utilización de la lengua del Estado para publicitar los servicios, o de la moneda para la realización de las transacciones comerciales o incluso la disponibilidad de una aplicación para móvil en la tienda de aplicaciones nacional²⁶. En este sentido, especifica el propio Reglamento que la mera accesibilidad de una interfaz en línea (como por ejemplo la accesibilidad de la página web del proveedor de servicios o de un intermediario, o de una dirección de correo electrónico y otros datos de contacto) en uno o más Estados miembros, considerada aisladamente, no constituiría condición suficiente para la aplicación del mismo²⁷.

Conscientes desde Europa de la importancia que la efectiva recepción de la Orden reviste para su cumplimiento y para el éxito de sus previsiones, paralelamente a la tramitación de esta propuesta de Reglamento, se iniciaron los trámites para aprobar una Directiva comunitaria que establezca la obligación de los proveedores de servicios de designar un representante legal en el país en el que los prestan²⁸. Designado así el representante legal será con él con quien entienda la autoridad emisora la Orden de entrega; si bien, en su defecto —ante la falta de designación—, se prevé la posibilidad de remitir la Orden a cualquier establecimiento del proveedor, en cualquier otro país de la Unión (art. 7.2 de la Propuesta de Reglamento). Debe hacerse notar, en todo caso, que la remisión de la Orden a un proveedor de servicios concreto ha de serlo en relación con servicios que éste haya ofrecido en el ámbito de la unión; con lo que no cabría dirigir una Orden de entrega de pruebas electrónicas a un proveedor de servicios establecido en la Unión, pero en relación con unos servicios ofertados y prestados fuera del ámbito de ésta²⁹.

En todo caso, la Abogacía Europea no ha aceptado con agrado la opción de escoger al proveedor de servicios como destinatario de la Orden. Su preocupación fundamental reside en que cuando se trate de datos sensible o de datos protegidos por algún privilegio reconocido, como pueda ser el secreto de las relaciones profesionales abogado-cliente, el procedimiento previsto por la Propuesta de Reglamento a partir del cual el Estado emisor debe consultar a la autoridad competente del Estado en el que se recabarán los datos puede no resultar del todo

se realiza la actividad de prestación de servicios o de una infraestructura estable a partir de la cual se gestiona la actividad” [art. 2 (5); nótese que, en el texto en Castellano, esta definición se encuentra en el art. 2 (4)].

²⁶ Cfr. Considerando 28.

²⁷ Cfr. Considerando 27.

²⁸ Actualmente en tramitación: 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. COM (2018) 216 Final; 2018/0107 (COD).

²⁹ Cfr. Considerando 26.

satisfactorio. En este sentido considera la Abogacía Europea que siempre que fuera posible, las Órdenes de entrega deberían remitirse directamente al Responsable de los datos que velaría con mayor garantía por la salvaguarda de los datos especialmente protegidos³⁰.

V. REQUISITOS OBJETIVOS DE LA ORDEN: PROPORCIONALIDAD Y NECESIDAD

La válida emisión de una Orden europea de entrega de pruebas electrónicas aparece condicionada al cumplimiento de los requisitos de proporcionalidad y necesidad de la medida, así como a la exigencia de que exista en el Estado emisor una medida similar para la misma infracción penal en una situación nacional comparable. Todas estas circunstancias³¹ deberán quedar debidamente acredita-

³⁰ En los comentarios previos emitidos por la Abogacía Europea a instancia de la Comisión, para la tramitación del texto legal que nos ocupa, puede leerse (p. 3) que las solicitudes de acceso a la prueba digital deben, cuando sea posible, dirigirse siempre a los responsables de datos, en lugar de a los proveedores de los mismos que, especialmente cuando los datos sean gestionados por un despacho de abogados, proporcionaría mejores garantías contra cualquier intercambio ilícito de información privilegiada https://www.cbbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf.

³¹ Junto a estas circunstancias, la Orden de entrega deberá hacer referencia también a todos aquellos datos que la propia lógica de su buen funcionamiento exige y que el art. 5 (5) se encarga de detallar: datos identificativos de la autoridad emisora así como de la autoridad validadora, cuando proceda; los datos del proveedor de servicios al que se dirigen y en su nombre, el de su representante legal (forma en la que entiendo que debería interpretarse la dicción literal del art. 5 (5. b) cuando establece que debe hacer constar “el destinatario de la orden europea de entrega a que se refiere el artículo 7”); las personas cuyos datos se solicitan (salvo cuando la única finalidad de la orden sea identificar a una persona); la categoría de los datos solicitados (datos de los abonados, datos relativos al acceso, datos de transacciones o datos de contenido); el periodo que abarca la solicitud de entrega; las razones que justifican la urgencia con se solicite la entrega en los especiales plazos contemplados para estos supuestos; y, por último, cuando la orden se refiera a datos almacenados o tratados como parte de una infraestructura facilitada por un proveedor de servicios a una empresa u otra entidad distinta de una persona física, la expresión de que las medidas no se han podido dirigir directamente contra la empresa o entidad, —tal y como prevé el Reglamento, como norma general— por considerar que, de ser así, podría ponerse en peligro la investigación. En mi opinión, no obstante, un recto entendimiento de esta exigencia pasa no sólo por hacer constar dicho extremo en la solicitud, sino por justificar en la misma los motivos concretos por los que se entiende que, de solicitarlo directamente a la empresa o entidad, correría peligro la investigación; sobre el tema me he ocupado con detalle en “Europa ante el reto...”, cit, p. 313.

das en la Orden si bien es de hacer notar que, especialmente respecto de la necesidad y proporcionalidad de la medida —y con el fin de no perjudicar el curso de la investigación—, su justificación no deberá incluirse en la presentación del certificado EPOC³² que se utilizará como instrumento formal para transmitir la Orden.

Efectivamente, la materialización de una Orden se realiza a través de la cumplimentación y entrega de los impresos normalizados (denominados, por sus siglas en Inglés, como EPOC —para las órdenes de entrega— y EPOC-PR —para las órdenes de conservación—) que se han hecho constar en los Anexos I y II a la Propuesta de Reglamento y que están previstos para agilizar y facilitar la tramitación de las solicitudes. Sólo cuando el destinatario de la Orden la incumpliera, la autoridad emisora remitirá a la autoridad judicial competente de ese Estado el Certificado EPOC, acompañado, en este caso, de la justificación de la proporcionalidad y necesidad de la medida a fin de iniciar los trámites de ejecución del mismo previstos en el propio Reglamento³³.

La exigencia de proporcionalidad puede analizarse desde dos perspectivas diferentes: desde la proporcionalidad, en general, de las previsiones normativas —es decir, analizando si, en general, se justifica la regulación de estas medidas de investigación para la consecución de los fines trazados— y desde la óptica del caso concreto y de los datos solicitados respecto del mismo. En tanto en cuanto, la primera opción ha sido expuesta con anterioridad al circunscribirla a tan sólo determinados supuestos delictivos en función del tipo de datos solicitado, se hará referencia a continuación a la exigencia de proporcionalidad en el caso concreto, que debe aparecer debidamente fundamentada —en los términos vistos— en la solicitud. La finalidad perseguida es garantizar el respeto a los derechos fundamentales y los principios reconocidos por la Carta de los Derechos Fundamentales de la Unión Europea³⁴. En este contexto, la posible afcción de tales derechos se dará cuando se pidan determinados datos de personas que constituyen la parte acusada de un proceso penal en curso; pero también cuando se afecten derechos

³² Vid. Art. 8.3 Propuesta de Reglamento.

³³ Art. 14 Propuesta de Reglamento.

³⁴ La posibilidad de limitar el ejercicio de los derechos y libertades previstos en la Carta de la Unión aparece contemplada en el art. 52.1 de la misma y sometida a los principios de proporcionalidad y necesidad, pero la inexistencia de una regulación específica sobre derechos fundamentales en el ámbito de la Unión Europea supondrá —como con acierto destaca ARMENTA— “que una eventual reclamación deberá sortear una situación ciertamente compleja en la que concurren la normativa europea, la jurisprudencia del TEDH y del TJUE, así como la interna de los diversos Tribunales Constitucionales”. ARMENTA DEU, T., “Orden Europea de Investigación y exclusión probatoria. Admisibilidad, impugnación y denegación en el Estado de enjuiciamiento o en el de ejecución cuando se aprecie vulneración de un derecho fundamental”, en *Orden europea de investigación y prueba transfronteriza en la unión europea*, GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019, p. 781.

de terceros que ni siquiera son parte en dicho proceso. La existencia, precisamente, de esta justificación de la proporcionalidad en el caso concreto permitirá articular los recursos e impugnaciones previstos para luchar contra la efectividad de una prueba que pueda haberse obtenido con vulneración de Derechos Fundamentales. Mientras que para quienes sean parte de un proceso, serán los mecanismos internos del Estado en que se tramite éste los que marquen las opciones procesales existentes para oponerse a esta prueba, quienes vean afectados sus derechos sin ser parte en proceso alguno podrán impugnar esa información, ilícitamente obtenida, a través de los mecanismos que se hayan previsto, en el Estado de emisión de la Orden³⁵.

Nótese, en todo caso, que el art. 11 (2) de la propuesta de Reglamento ha establecido la obligación de informar sin demora a la persona cuyos datos se solicitan. Ello no obstante, la posibilidad de suspender la puesta en conocimiento de este hecho durante “el tiempo que sea necesario y proporcionado para evitar la obstrucción del proceso penal” puede abrir una vía de conflicto con el derecho a un juicio justo. Es por ello que la Abogacía Europea ha considerado que “la imposición de restricciones de confidencialidad a las EPO debe estar sujeta a la aprobación de una autoridad judicial independiente y, en cada caso, estar debidamente motivada y justificada por la autoridad emisora sobre la base de evaluaciones significativas y documentadas”³⁶.

Siguiendo la consolidada doctrina del TC español, la ponderación de la proporcionalidad de una medida limitativa de derechos fundamentales exige la valoración de tres aspectos fundamentales que constituyen lo que se ha dado en

³⁵ En este sentido, clarifica el Considerando 54 de la Propuesta de Reglamento que “Es esencial que todas las personas cuyos datos se solicitan en investigaciones o procesos penales tengan acceso a una tutela judicial efectiva, de conformidad con el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea. Para los sospechosos y acusados, el derecho a una tutela judicial efectiva deberá ejercerse durante el proceso penal. Esto puede afectar a la admisibilidad, o en su caso al peso en el proceso, de las pruebas obtenidas por estos medios. Asimismo, se beneficiarán de todas las garantías procesales aplicables a ellos, como el derecho a la información. También las personas que no sean sospechosos o acusados deberán tener derecho a la tutela judicial efectiva. Por tanto, como mínimo, deberá preverse la posibilidad de impugnar la legalidad de una orden europea de entrega, en particular su necesidad y proporcionalidad. El presente Reglamento no deberá limitar los posibles motivos para impugnar la legalidad de la orden. Estos recursos deberán ejercerse en el Estado emisor con arreglo a su legislación nacional”.

³⁶ CCBE Preliminary comments on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Punto 6 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf.

llamar el “triple filtro” constitucional: la “idoneidad de la medida” o su adecuación concreta para conseguir el objetivo propuesto; la “necesidad” de la misma, en el sentido de no existir otra medida menos lesiva para el logro de esa misma finalidad; y, por último, la “proporcionalidad en sentido estricto” o balance entre las superiores ventajas que debe representar dicha medida respecto del interés general, frente a los posibles perjuicios concretos sobre determinados bienes o valores³⁷. La justificación de la proporcionalidad de la medida, en una Orden europea de entrega de pruebas electrónicas deberá hacer referencia a todos y cada uno de los extremos —o filtros— referidos entendiendo pues, la proporcionalidad en un sentido amplio, en el que se incluye también la valoración de su “necesidad”.

Pero en la delimitación de los requisitos objetivos a tener en cuenta para la válida emisión de una Orden de entrega, se exige también que en el Estado de emisión haya prevista una medida similar para la investigación del hecho delictivo. La justificación de este extremo exige hacer constar en la Orden, además de todo lo anterior, las disposiciones de Derecho penal aplicables del Estado emisor (art. 5.5.f).

Sin embargo, como con acierto ha resaltado la Abogacía Europea en relación con la proporcionalidad de la medida es cierto que entre las condiciones para emitir una Orden Europea de Entrega o Conservación no se incluye ningún umbral de suficiente grado de sospecha (*vid.*, artículo 5). Es por ello que, en su opinión y para evitar posibles abusos, el texto normativo definitivo debería reflejar expresamente que las órdenes de entrega solo podrán ser validadas por las autoridades competentes si existen razones apremiantes que den lugar a un grado suficiente de sospecha que justifique la confiscación transfronteriza de datos³⁸.

VI. BIBLIOGRAFÍA

ARMENTA DEU, T., “Orden Europea de Investigación y exclusión probatoria. Admisibilidad, impugnación y denegación en el Estado de enjuiciamiento o en el de ejecución cuando se aprecie vulneración de un derecho fundamental”, en *Orden europea de investigación y prueba transfronteriza en la unión europea*, GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019.

³⁷ Por todas, STC 96/2012, de 7 de mayo (RTC 2012, 96).

³⁸ CCBE Preliminary comments on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Punto 3 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf.

- ARRABAL PLATERO, P., “La videovigilancia laboral cómo prueba en el proceso”, *Revista General de Derecho procesal*. Iustel, nº 37, 2015.
- ARRABAL PLATERO, P., *La prueba tecnológica. Aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019.
- BUENO DE MATA, F., *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, 2019.
- FUENTES SORIANO, O., “Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las Órdenes europeas de entrega y conservación de pruebas electrónicas”, *Era Digital, Sociedad y Derecho* (Dir. FUENTES SORIANO O.), Tirant lo Blanch, Valencia, 2020.
- FUENTES SORIANO, O., “La intervención de las comunicaciones tecnológicas tras las reformas de 2015” en ALONSO CUEVILLAS SAYROL (Dir.), *El nuevo proceso penal tras las reformas de 2015*, Atelier y Fundación privada Manuel Serra Domínguez, 2016.
- FUENTES SORIANO, O., “Comunicaciones telemáticas: práctica y valoración de la prueba”, en *El proceso penal. Cuestiones fundamentales* (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017
- GÓMEZ AMIGO, L., “Nuevas perspectivas para la obtención transfronteriza de prueba penal electrónica en la Unión Europea”, *Diario La Ley*, nº 9340, de 18 de enero de 2019
- GÓMEZ AMIGO, L., “Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima”, *Revista Española de Derecho Europeo*, nº 71, julio-septiembre 2019.
- GÓMEZ AMIGO, L., “Prueba electrónica en la Unión europea: Las futuras órdenes europeas de entrega y conservación”, en *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, (GONZÁLEZ CANO. Dir.), Tirant lo Blanch, Valencia, 2019.
- LARO GONZÁLEZ, M.E., “Derechos y garantías del menor en el proceso penal. Armonización legislativa y necesidades procesales”, *La Ley Unión Europea*, Nº 73, 30 de septiembre de 2019.
- MONTORO SÁNCHEZ, J.A., “Breve análisis acerca del futuro Reglamento Comunitario “E-Evidence” sobre las órdenes europeas de conservación y entrega de pruebas y evidencias electrónicas a efectos de enjuiciamiento penal”, en *Orden europea de investigación y prueba transfronteriza en la unión europea*, GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019.
- ORMAZÁBAL SÁNCHEZ, G., “El tortuoso camino hacia la construcción del espacio judicial europeo en materia penal. Algunas consideraciones en torno al reconocimiento mutuo de pruebas, la euroorden y la Fiscalía Europea”, en *Derecho y proceso. Liber Amicorum del Profesor Francisco Ramos Méndez* (CACHÓN CADENAS y FRANCO ARIAS, Coords.), Barcelona, 2018.
- PÉREZ MARÍN, M.A., *La lucha contra la criminalidad en la Unión Europea. El camino hacia una jurisdicción penal común*, Atelier, Barcelona, 2013.
- RODRÍGUEZ ÁLVAREZ, A., “Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de enjuiciamiento criminal” en *Justicia penal*

y nuevas formas de delincuencia, (Dir. ASECIO MELLADO; Coord. FERNÁNDEZ LÓPEZ), Tirant lo Blanch, Valencia, 2017.