LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS PENALES ELECTRÓNICAS: UNA REGULACIÓN QUE SE APROXIMA[1]

European production and preservation orders for electronic evidence in criminal matters: an incoming regulation

LUIS GÓMEZ AMIGO

Catedrático de Derecho Procesal. Universidad de Almeria

Revista Española de Derecho Europeo 71
Julio – Septiembre 2019
Págs. 23–56

SUMARIO: I. PLANTEAMIENTO. II. EVOLUCIÓN DE LA ESTRATEGIA EUROPEA EN MATERIA DE ACCESO TRANSFRONTERIZO A LAS PRUEBAS PENALES ELECTRÓNICAS. III. LA PROPUESTA DE REGLAMENTO SOBRE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS ELECTRÓNICAS A EFECTOS DE ENJUICIAMIENTO PENAL. 1. *Finalidad y ámbito de aplicación de las órdenes europeas de entrega y conservación*. 2. *Autoridades emisoras, condiciones de emisión y certificados de las órdenes europeas de entrega y conservación*. 3. *Cumplimiento de las órdenes europeas de entrega y conservación por los proveedores de servicios*. 4. *Trámite de reconocimiento y ejecución por la autoridad competente del Estado de ejecución, y motivos de denegación*. 5. *Procedimientos de reexamen y recursos*. IV. LAS NEGOCIACIONES PARA UN ACUERDO ENTRE LA UNIÓN EUROPEA Y LOS ESTADOS UNIDOS DE AMÉRICA SOBRE EL ACCESO TRANSFRONTERIZO A LAS PRUEBAS PENALES ELECTRÓNICAS. V. VALORACIÓN FINAL.

1. Estudio realizado en el Marco del Proyecto de Investigación, "Asignaturas pendientes del sistema procesal español" (DER2017-83125-P), Ministerio de Economía, Industria y Competitividad (Gobierno de España); cofinanciado con FEDER.

RESUMEN: En este trabajo se estudia la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, de 17 de abril de 2018. Estas órdenes europeas pretenden ser un nuevo instrumento de reconocimiento mutuo en materia penal en la Unión Europea, para la obtención transfronteriza de pruebas electrónicas. Con ellas, la autoridad competente del Estado emisor podrá ordenar directamente a un proveedor que ofrezca servicios de comunicaciones electrónicas y de la sociedad de la información en la Unión Europea que entregue o conserve pruebas penales electrónicas de las que disponga, interviniendo la autoridad competente del Estado de ejecución sólo en caso de incumplimiento por el proveedor de servicios, para adoptar las medidas necesarias para la ejecución de las órdenes.

PALABRAS CLAVE: Orden europea de entrega– Orden europea de conservación– Pruebas electrónicas– Reconocimiento mutuo en materia penal

ABSTRACT: This paper studies the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, on April 17, 2018. These European Orders intend to be a new instrument of mutual recognition in criminal matters in the European Union for cross-border access to electronic evidence. Through them, the competent authority of the issuing State may directly order to a provider who offers electronic communications and information society services in the European Union to produce or preserve electronic criminal evidence. The competent authority of the enforcing State will intervene only if the service provider does not comply the European Order, to carry on the necessary measures for its execution.

KEYWORDS: European Production Order– European Preservation Order– Electronic Evidence– Mutual Recognition in Criminal Matters

Fecha de recepción: 20-3-2019
Fecha de aceptación: 3-4-2019

I. PLANTEAMIENTO

Con la promulgación de 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 (en adelante, OEI), se produce un avance fundamental en materia de obtención de prueba penal transfronteriza en el ámbito de la Unión Europea. En cuanto al ordenamiento español, la incorporación de la OEI se realiza en virtud de la reforma de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea (en adelante, LRM), operada por la Ley 3/2018, de 11 de junio, que introduce la OEI como nuevo instrumento de reconocimiento mutuo en materia penal en el Título X de la LRM (arts. 186 –223), en sustitución del exhorto europeo de obtención de pruebas.

La OEI viene a sustituir, en las relaciones entre los Estados miembros a los que les es aplicable[2], al sistema anterior de obtención de prueba penal transfronteriza[3], de carácter disperso y fragmentario, que incluía tanto instrumentos de asistencia judicial (Convenio europeo de asistencia judicial en

2. Conforme a los Considerandos 44 y 45, la Directiva sobre la OEI no se aplica ni a Irlanda ni a Dinamarca.
3. Así lo dispone el art. 34 de la Directiva sobre la OEI.

materia penal de 20 de abril de 1959, Convenio de aplicación del Acuerdo de Schengen de 19 de junio de 1990 y Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 29 de mayo de 2000) como de reconocimiento mutuo (Decisión Marco 2003/577/JAI del Consejo, de 22 de julio de 2003, relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y de aseguramiento de pruebas; y Decisión Marco 2008/978/JAI del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal)[4].

Como hemos señalado, la OEI supone un destacado avance frente a los anteriores instrumentos de reconocimiento mutuo, ya que el exhorto europeo de obtención de pruebas (Decisión Marco 2008/9789/JAI) sólo permitía la entrega de pruebas ya existentes, pero no su obtención; mientras que las resoluciones de embargo preventivo con el fin de aseguramiento de pruebas (Decisión Marco 2003/577/JAI) debían ir acompañadas de una solicitud por separado de transferencia de la prueba, presentada de conformidad con el sistema de asistencia judicial penal.

Frente a ello, la Directiva sobre la OEI establece un sistema ágil y rápido para la obtención y traslado entre los Estados miembros de cualquier tipo de prueba (con excepción de la creación de equipos conjuntos de investigación y la obtención de pruebas en dichos equipos)[5], aplicable tanto a las medidas de investigación propias de la instrucción como a pruebas en sentido estricto, y abarcando la obtención de prueba y también el traslado de pruebas que ya obren en poder de las autoridades del Estado de ejecución, así como las medidas de aseguramiento de la prueba. La eficacia y agilidad de este nuevo instrumento de reconocimiento mutuo[6] se consigue configurando la OEI como una

4. La Directiva sobre la OEI sustituye a las disposiciones correspondientes de los Convenios y a las Decisiones Marco. La sustitución de la Decisión Marco 2003/577/JAI por la Directiva sobre la OEI es parcial, pues sólo se produce en relación con el aseguramiento de pruebas. Posteriormente, se ha dictado el Reglamento (UE) 2018/1805 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso, que también sustituye a las disposiciones de la Decisión Marco 2003/577/JAI en lo referente al embargo de bienes entre los Estados miembros vinculados por el Reglamento, a partir del 19 de diciembre de 2020. Además, el Reglamento (UE) 2016/95, de 20 de enero de 2016, ha derogado la Decisión Marco 2008/978/JAI.
5. Así lo dispone el art. 3 de la Directiva sobre la OEI. Al respecto, téngase en cuenta la Decisión Marco 2002/465/JAI del Consejo, de 13 de junio de 2002, sobre equipos conjuntos de investigación. Conforme al Considerando 9, la Directiva sobre la OEI tampoco se aplica a la vigilancia transfronteriza a la que se refiere el Convenio de aplicación del Acuerdo de Schengen.
6. El principio de reconocimiento mutuo puede ser insuficiente en cuanto a la admisibilidad de la prueba en el Estado de ejecución, por lo que debería complementarse con unas normas europeas comunes mínimas en materia de obtención de prueba. Cfr. en este sentido, ORMAZABAL SÁNCHEZ, G., "El tortuoso camino hacia la construcción del espacio

resolución judicial que se transmite directamente entre autoridades judiciales (u otras autoridades competentes para la investigación en procesos penales, requiriéndose en este caso la validación de la OEI por una autoridad judicial), por medio de formularios, debiendo ser reconocida y ejecutada en el Estado de ejecución, salvo que concurran una serie de motivos tasados de denegación, y estableciéndose plazos breves para el reconocimiento y la ejecución de la OEI[7].

De manera especial a partir de los atentados terroristas de París de noviembre de 2015 y Bruselas de marzo de 2016, la Unión Europea ha establecido como una de sus prioridades esenciales en materia penal facilitar la obtención de pruebas electrónicas de carácter transfronterizo, esenciales para poder investigar, y así evitar y perseguir de manera eficaz los delitos graves, en especial, los atentados terroristas. Téngase en cuenta, además, que a menudo las redes sociales y los servicios de correo electrónico y de mensajería instan-

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, M. y FRANCO ARIAS, J., Coordinadores), Barcelona, 2018, vol. III, p. 1805. Sin embargo, ésta es una cuestión que sigue pendiente desde su planteamiento por el *Libro Verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad*, de 11 de noviembre de 2009, COM(2009) 624 final.

7. Sobre el tema y desde una perspectiva general, pueden verse AGUILERA MORALES, "La Orden Europea de Investigación: nuevas atribuciones para el Ministerio Fiscal", *Justicia*, 2018-2 pp. 195-221; ARANGÜENA FANEGO, C., "Orden europea de investigación: próxima implementación en España del nuevo instrumento de obtención de prueba penal transfronteriza", *Revista de Derecho Comunitario Europeo*, núm. 58, septiembre-diciembre 2017, pp. 905-939; BACHMAIER WINTER, L., "Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigación", *Revista General de Derecho Europeo*, núm. 36, 2015, pp. 1-35; DOMÍNGUEZ RUIZ, L., "La orden europea de investigación: el camino hacia un régimen europeo uniforme en materia de prueba penal", en *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales* (JIMÉNEZ CONDE, F., Director), Valencia, 2018, pp. 337-345; GRANDE SEARA, P., "Reconocimiento y ejecución en España de una Orden Europea de Investigación", en *Integración europea y justicia penal* (GONZÁLEZ CANO, M.ª I., Directora), Valencia, 2018, pp. 435-481; JIMENO BULNES, M., "Orden europea de investigación en materia penal", en *Aproximación legislativa versus reconocimiento mutuo en el desarrollo del espacio judicial europeo: una perspectiva multidisciplinar* (JIMENO BULNES, M., Directora), Barcelona, 2016, pp. 151-208; MARTÍN GARCÍA, A. L. y BUJOSA VADELL, L., *La obtención de prueba en materia penal en la Unión Europea*, Barcelona, 2016; MARTÍNEZ GARCÍA, E., *La orden europea de investigación. Actos de investigación, ilicitud de la prueba y cooperación judicial transfronteriza*, Valencia, 2016 y "La orden europea de investigación", en *Integración europea y justicia penal* (GONZÁLEZ CANO, M.ª I., Directora), Valencia, 2018, pp. 404-434; RODRÍGUEZ-MEDEL NIETO, C., *Obtención y admisibilidad en España de la prueba penal transfronteriza. De las comisiones rogatorias a la orden europea de investigación*, Cizur Menor (Navarra), 2016; ROMERO PRADAS, M.ª I., "La prueba penal en Europa, una cuestión compleja. La orden europea de investigación como nuevo instrumento de obtención de pruebas en procesos penales transnacionales y su próxima incorporación al Derecho español", en *Integración europea y justicia penal* (GONZÁLEZ CANO, M.ª I., Directora), Valencia, 2018, pp. 343-401; y los trabajos contenidos en la obra colectiva dirigida por GONZÁLEZ CANO, M.ª I., *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Valencia, 2019.

tánea son el único lugar donde los investigadores pueden hallar pistas para investigar el delito y pruebas para enjuiciarlo. Es verdad que la Directiva sobre la OEI cubre todas las medidas de investigación, incluido el acceso a las pruebas electrónicas, pero no contiene disposiciones específicas sobre este tipo de pruebas. Por ello, estas pruebas pueden seguir obteniéndose a través de la OEI, pero la Unión ya ha presentado una iniciativa legislativa para establecer instrumentos de reconocimiento mutuo con esa finalidad de obtener pruebas penales electrónicas en otro Estado miembro, que se adapte mejor a las particularidades de esta clase de pruebas: la orden europea de entrega y la orden europea de conservación[8]. Se trata de 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*, de 17 de abril de 2018[9].

En efecto, la prueba penal electrónica presenta características especiales. Los servicios de comunicaciones electrónicas y los servicios de la sociedad de la información (redes sociales, por ejemplo) pueden prestarse desde cualquier lugar del mundo y no exigen una infraestructura física ni empresarial en el Estado miembro en el que se ofrece el servicio, y normalmente el almacenamiento de datos no está ubicado en dicho Estado miembro. De manera que las autoridades de los Estados miembros necesitan acceder a datos que pueden servir de prueba y que están almacenados fuera de su país o por proveedores de servicios de otros Estados miembros o de terceros países.

Con esta iniciativa legislativa[10], se pretenden establecer instrumentos penales de reconocimiento mutuo adaptados al carácter volátil y la dimensión transfronteriza de las pruebas electrónicas, de manera que una autoridad judicial de un Estado miembro pueda ordenar a un proveedor que ofrezca servicios de

8. Puede verse una primera aproximación a este tema en GÓMEZ AMIGO, L., "Nuevas perspectivas para la obtención transfronteriza de prueba penal electrónica en la Unión Europea", *Diario La Ley*, núm. 9340, de 18 de enero de 2019. Véanse asimismo, del mismo autor, "Prueba penal electrónica en la Unión Europea: las futuras órdenes europeas de entrega y conservación", y MONTORO SÁNCHEZ, "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", ambos en *Orden europea de investigación y prueba transfronteriza en la Unión Europea* (GONZÁLEZ CANO, M.ª I., Directora), Valencia, 2019, pp. 157 y ss., y 171 y ss., respectivamente.
9. COM(2018) 225 final.
10. Para conocer mejor el contexto en que surge y su finalidad, puede consultarse la Exposición de Motivos de la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas penales electrónicas, que contiene una explicación detallada de los preceptos contenidos en la Propuesta. Véase también el documento técnico de los Servicios de la Comisión, *Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace*, de 22 de mayo de 2017 (9554/17). A nivel divulgativo, puede resultar interesante la consulta de la *Factsheet* (ficha técnica) *e-evidence*, en el sitio web de la Comisión Europea:
http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm

comunicaciones electrónicas y de la sociedad de la información en la Unión[11] que entregue o conserve pruebas electrónicas, a través de una orden europea de entrega o de una orden europea de conservación. Y es que una de las novedades más relevantes de esta iniciativa legislativa reside en que las órdenes europeas de entrega y conservación no se dirigen a una autoridad del Estado de ejecución, sino directamente al proveedor de servicios establecido o representado en otro Estado miembro, que es el que deberá cumplirlas, interviniendo sólo la autoridad competente del Estado de ejecución en caso de incumplimiento por el proveedor de servicios, adoptando aquélla las medidas necesarias para su ejecución. Téngase en cuenta que esta Propuesta de Reglamento sólo se aplica a los datos almacenados, mientras que la interceptación instantánea de las telecomunicaciones no está cubierta por la presente Propuesta[12].

Con carácter complementario a la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación y en la misma fecha, la Unión Europea ha presentado otra iniciativa legislativa: 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*, de 17 de abril de 2018[13]. En ella, se establece la obligación de que los proveedores de servicios[14] designen un representante legal en la Unión para la recepción, el cumplimiento y la ejecución de las resoluciones y ordenes emitidas por las autoridades competentes de los Estados miembros a efectos de recabar pruebas para procesos penales. Con ello, se consigue que exista siempre un claro destinatario de dichas resoluciones y órdenes, y se facilita a los proveedores de servicios el cumplimiento de las mismas, ya que será el representante legal el responsable de recibir y cumplir las resoluciones y órdenes en nombre del proveedor de servicios[15].

II. EVOLUCIÓN DE LA ESTRATEGIA EUROPEA EN MATERIA DE ACCESO TRANSFRONTERIZO A LAS PRUEBAS PENALES ELECTRÓNICAS

Ya desde el año 2015 la Comisión considera prioritaria una estrategia común europea en materia de acceso transfronterizo a la prueba penal elec-

11. Concretamente, se trata de proveedores de servicios de comunicaciones electrónicas, proveedores de servicios de la sociedad de la información y proveedores de servicios de asignación de nombres de dominio de internet y de direcciones IP.
12. En cambio, la intervención de las telecomunicaciones sí está prevista en los arts. 30 y 31 de la Directiva sobre la OEI. Sobre este concreto tema, véase GONZÁLEZ MONJE, A., *Cooperación jurídica internacional en materia penal e intervención de las comunicaciones como técnica especial de investigación*, Granada, 2017.
13. COM(2018) 226 final.
14. Igual que en la iniciativa legislativa anterior, se trata de proveedores de servicios de comunicaciones electrónicas, proveedores de servicios de la sociedad de la información y proveedores de servicios de asignación de nombres de dominio de internet y de direcciones IP.
15. Sobre su contexto y finalidad, véase la Exposición de Motivos de la Propuesta de Directiva para la designación de representantes legales a efectos de recabar pruebas penales electrónicas, que contiene una explicación detallada de los preceptos contenidos en la Propuesta.

trónica, que garantice su admisibilidad ante los tribunales, y así lo manifestó en la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Agenda Europea de Seguridad*, de 28 de abril de 2015[16]. En este primer momento la estrategia se plantea como una medida necesaria para luchar contra la ciberdelincuencia, enfoque que se mantiene en la Resolución del Parlamento Europeo, de 3 de octubre de 2017*, sobre la lucha contra la ciberdelincuencia*[17]. En esta resolución, el Parlamento Europeo solicita a la Comisión que presente una propuesta legislativa que posibilite la obtención transfronteriza, de manera eficaz y rápida, de pruebas penales electrónicas, y que incorpore las disposiciones necesarias para facilitar la admisibilidad de las pruebas electrónicas ante los tribunales. El nuevo sistema se articularía sobre la OEI, adaptando su régimen a las especialidades de las pruebas electrónicas.

La preocupación por instaurar un sistema europeo eficaz para la prueba penal electrónica se mantiene constante, manifestándose en los sucesivos Informes de la Comisión sobre una Unión de la Seguridad genuina y efectiva[18]; en el Programa de trabajo de la Comisión para 2018[19]; y en las prioridades legislativas de la Unión Europea para 2018-2019, recogiéndose entre las 31 propuestas legislativas presentadas por la Comisión como objeto de un trato prioritario por el Parlamento Europeo y el Consejo[20]. Por último, figura en el Programa de trabajo de la Comisión para 2019, entre las propuestas prioritarias pendientes, dentro del ámbito de actuación *Un espacio de justicia y derechos fundamentales basado en la confianza mutua*[21].

16. COM(2015) 185 final.
17. DOUE C 346, de 27 de septiembre de 2018, pp. 29 y ss.
18. *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Duodécimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva*, de 12 de diciembre de 2017, COM(2017) 779 final; *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Decimocuarto informe de situación hacia una Unión de la Seguridad genuina y efectiva*, de 17 de abril de 2018, COM(2018) 211 final; *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Decimosexto Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva*, de 10 de octubre de 2018, COM(2018) 690 final; *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Decimoséptimo Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva*, de 11 de diciembre de 2018, COM(2018) 845 final; *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Decimoctavo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva*, de 20 de marzo de 2019, COM(2019) 145 final.
19. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Programa de trabajo de la Comisión para 2018*, de 24 de octubre de 2017, COM(2017) 650 final.
20. *Una Europa más unida, más fuerte y más democrática: Declaración conjunta sobre las prioridades legislativa de la Unión Europea para 2018-2019*, Comunicado de prensa de la Comisión Europea de 14 de diciembre de 2017.
21. Cfr. el Anexo III de la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Programa de trabajo de la*

El enfoque inicial centrado en la lucha contra la ciberdelincuencia se corrige posteriormente, diseñándose la estrategia europea en materia de prueba electrónica transfronteriza como un instrumento para luchar contra la delincuencia grave, especialmente los delitos de terrorismo. En definitiva, lo relevante no es tanto que los delitos se comentan a través de las nuevas tecnologías de la información y la comunicación, sino poder utilizar las fuentes de prueba que estas nuevas tecnologías proporcionan[22].

Ese es el enfoque que finalmente sigue la Comisión en sus Propuestas de 17 de abril de 2018, de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas penales electrónicas, y de Directiva para la designación de representantes legales a efectos de recabar pruebas penales electrónicas, abandonándose la idea originaria de basar el sistema sobre la OEI, que pasa a articularse sobre dos nuevos instrumentos de reconocimiento mutuo: la orden europea de entrega y la orden europea de conservación.

Las Propuestas de Reglamento y Directiva de 17 de abril de 2018 se acompañaron con el *Documento de trabajo de los Servicios de la Comisión: Evaluación de impacto*, también de 17 de abril de 2018[23], y el 12 de julio de 2018 el Comité Económico y Social Europeo emitió Dictamen sobre las mismas[24]. Existe una segunda versión de la Propuesta de Reglamento sobre las órdenes europeas

---

Comisión para 2019. Cumplir lo prometido y preparados para el futuro, de 23 de octubre de 2018, COM(2018) 800 final.

22. "*Al tiempo que crece el uso de las redes sociales, el correo electrónico, los servicios de mensajería y las aplicaciones para comunicarse, trabajar, socializar y obtener información, incluso con fines ilegítimos, aumentan también los flujos transfronterizos de datos. Consecuentemente, un número cada vez mayor de investigaciones penales se apoya en pruebas electrónicas que no son accesibles al público. La naturaleza carente de fronteras de internet y el modo en que pueden prestarse servicios desde cualquier parte del mundo, también por empresas que no sean europeas, hacen que facilitar el acceso transfronterizo a las pruebas electrónicas se haya convertido en una cuestión acuciante para casi cualquier tipo de infracción. En concreto, los recientes atentados terroristas han puesto de relieve la necesidad, prioritaria, de encontrar herramientas para que los fiscales y jueces de los Estados miembros de la Unión Europea obtengan las pruebas electrónicas de manera más rápida y eficaz.*
Más de la mitad de las investigaciones penales actuales requieren del acceso a pruebas electrónicas transfronterizas. Las pruebas electrónicas se necesitan en cerca del 85 % de las investigaciones penales, y, en dos tercios de estas investigaciones, es preciso obtener pruebas de proveedores de servicios en línea establecidos en otra jurisdicción. El número de solicitudes a los principales proveedores de servicios en línea aumentó un 84 % en el período comprendido entre 2013 y 2018. Estos tipos de datos son fundamentales en las investigaciones penales para identificar a una persona u obtener información sobre su actividad" [Exposición de Motivos, epígrafe 1: "*Contexto*", de 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 2019, COM(2019) 70 final].
23. SWD(2018)119 final. La versión íntegra se encuentra disponible únicamente en lengua inglesa. En castellano puede consultarse un Resumen de la Evaluación de impacto, que es una versión muy reducida del original.
24. DOUE C 367, de 10 de octubre de 2018, pp. 88 y ss.

de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, de 4 de marzo de 2019, sólo en versión española y que incorpora una mínima corrección de errores: en la versión original española, las definiciones del art. 2 estaban numeradas incorrectamente, del 1 al 14, ya que en las dos primeras definiciones estaba repetido el mismo ordinal, numerándose del 1 al 15 en la versión corregida[25].

El último paso de la Unión Europea en materia de prueba penal electrónica no se refiere al acceso transfronterizo a dicha clase de pruebas entre sus Estados miembros, sino en relación con terceros Estados. Al respecto, en la misma fecha, 5 de febrero de 2019, la Comisión Europea ha presentado dos nuevas iniciativas. Por una parte, 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*[26]. Y la *Recomendación de Decisión del Consejo por la que se autoriza la participación en las negociaciones de un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (STE núm. 185)*[27].

Aunque trataremos específicamente más adelante las negociaciones para alcanzar un acuerdo con los Estados Unidos de América, debemos señalar ahora que los Estados miembros de la Unión Europea no sólo necesitan un sistema eficaz de acceso a las pruebas penales electrónicas en relación con otros Estados miembros, sino también con los Estados Unidos, puesto que los principales proveedores de servicios en cuyo poder obran las pruebas penales electrónicas operan sujetos a la jurisdicción de este país. Por ello, se pretende lograr un acuerdo sobre el acceso transfronterizo a las pruebas penales electrónicas, acceso directo a través de los proveedores de servicios y que permita abordar los posibles conflictos de leyes entre los Estados miembros de la Unión Europea y los Estados Unidos de América. Además, este acuerdo debe ser compatible con las iniciativas en materia de acceso transfronterizo a la prueba penal electrónica de la Unión Europea, es decir, las Propuestas de Reglamento y Directiva objeto de estudio del presente trabajo.

El *Convenio del Consejo de Europa sobre Ciberdelincuencia*, hecho en Budapest el 23 de noviembre de 2001[28], tiene por objeto facilitar la persecución de

25. Otra iniciativa legislativa relacionada con las que se examinan en este trabajo es la *Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea*, de 12 de septiembre de 2018, COM(2018) 640 final, que, entre otras medidas, prevé que la autoridad competente pueda emitir una orden de retirada dirigida al prestador de servicios de alojamiento de datos para que éste retire contenidos terroristas o bloquee el acceso a ellos.
26. COM(2019) 70 final.
27. COM(2019) 71 final.
28. STE (Serie de Tratados Europeos) núm. 185. Instrumento de Ratificación por España de 20 de mayo de 2010 (BOE núm. 226, de 17 de septiembre de 2010).

los delitos cometidos por medio de un sistema informático. Posteriormente, se acordó el *Primer Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*, hecho en Estrasburgo el 28 de enero de 2003[29]. Desde hacía tiempo, las Partes en el Convenio sobre Ciberdelincuencia venían denunciando dificultades en el acceso a las pruebas electrónicas necesarias para la investigación y persecución de los delitos cometidos por medio de sistemas informáticos. Por ello, la Unión Europea pretende participar en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia, que mejore, entre otros aspectos, el acceso transfronterizo a la prueba penal electrónica en este tipo de delitos.

Por lo que a este tema se refiere, según la Comisión Europea, las negociaciones sobre el Segundo Protocolo adicional deberían contener disposiciones para hacer más eficaz la asistencia jurídica mutua, en particular, sobre las órdenes de entrega internacionales; disposiciones que permitan la cooperación directa con los proveedores de servicios en otras jurisdicciones con respecto a las solicitudes de información sobre los abonados, las solicitudes de conservación y los procedimientos de urgencia para la tramitación de las solicitudes; un marco más claro y salvaguardas más sólidas en cuanto a las prácticas existentes de acceso transfronterizo a los datos; y salvaguardas, incluidos los requisitos de protección de datos[30].

Además, el Segundo Protocolo adicional debe ser compatible con las propuestas legislativas de la Comisión sobre pruebas penales electrónicas, en particular, el Segundo Protocolo adicional debe reducir en la mayor medida de lo posible los riesgos de que las órdenes de entrega emitidas en el marco de un futuro instrumento de la Unión Europea sean contradictorias con las legislaciones de terceros países que sean Partes en este Protocolo[31]. Y ha de garantizarse que el Segundo Protocolo adicional contenga una cláusula de desconexión que establezca que los Estados de la Unión Europea sigan aplicando, en sus relaciones mutuas, la normativa de la Unión y no el Sergundo Protocolo adicional[32]. Finalmente, en las relaciones bilaterales entre los Estados Unidos de América y la Unión Europea, debe prevalecer el Acuerdo (en negociación) entre estas partes sobre el acceso transfronterizo a las pruebas penales electró-

---

Actualmente, son Partes en el Convenio 62 países, incluidos los Estados miembros de la Unión Europea, excepto Irlanda y Suecia.

29. STE núm. 189. Instrumento de Ratificación por España de 11 de noviembre de 2014 (BOE núm. 26, de 30 de enero de 2015).
30. Cfr. el Considerando 2 de la Recomendación de Decisión del Consejo sobre un Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia.
31. Cfr. el Anexo de la Recomendación de Decisión del Consejo sobre un Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia, letra c).
32. Cfr. el Anexo de la Recomendación de Decisión del Consejo sobre un Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia, letra d).

nicas sobre cualquier acuerdo o arreglo alcanzado en las negociaciones sobre el Segundo Protocolo adicional, en la medida en que regule las mismas cuestiones[33].

III. LA PROPUESTA DE REGLAMENTO SOBRE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS ELECTRÓNICAS A EFECTOS DE ENJUICIAMIENTO PENAL

1. FINALIDAD Y ÁMBITO DE APLICACIÓN DE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN

Atendiendo a su objeto (art. 1), la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación regula las ordenes que la autoridad de un Estado miembro puede dirigir, con carácter vinculante, a un proveedor que ofrezca servicios en la Unión y esté establecido o representado en otro Estado miembro, para que entregue pruebas penales electrónicas (orden europea de entrega) o las conserve de cara a una solicitud de entrega subsiguiente (orden europea de conservación), con independencia de la ubicación de los datos. En cualquier caso, las órdenes europeas de entrega y conservación serán compatibles con la OEI, pues los Estados miembros pueden seguir emitiendo una OEI para la obtención de pruebas penales electrónicas (art. 23).

Conforme a su ámbito de aplicación, las órdenes europeas de entrega y conservación sólo pueden emitirse en el ámbito de investigaciones o procesos penales sobre infracciones penales determinadas, "*tanto durante las fases previas al juicio como durante la fase procesal*[34]". También pueden ser emitidas en procesos relativos a infracciones penales por las que una persona jurídica pueda ser considerada responsable o ser castigada en el Estado emisor (art. 3.2). Y su objeto es obtener la entrega o conservación de pruebas electrónicas, entendidas éstas como las pruebas almacenadas en formato electrónico por un proveedor de servicios o en nombre del mismo en el momento de recepción de la orden de entrega o de conservación, consistentes en datos almacenados de diverso tipo: datos de los abonados, datos relativos al acceso, datos de transacciones y datos de contenido (art. 2.6)[35].

---

33. Cfr. la Exposición de Motivos de la Recomendación de Decisión del Consejo sobre un Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia, epígrafe 3: "*Disposiciones relevantes en la misma política sectorial*".
34. Según la explicación del artículo 3, "*la vinculación con una investigación específica distingue estas órdenes de las medidas preventivas o de las obligaciones de conservación de datos establecidas por ley, y garantiza la aplicación de los derechos procesales aplicables en los procesos penales. La competencia para iniciar investigaciones respecto de una infracción específica constituye, por tanto, una condición necesaria para la aplicación del Reglamento*" (Exposición de Motivos de la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación).
35. Según BUENO DE MATA, es primordial determinar qué se entiende realmente por *prueba electrónica*, "*observando no sólo su parte puramente electrónica sino aglutinando al mismo*

Por otra parte, sólo pueden dirigirse estas órdenes europeas a proveedores que ofrezcan sus servicios en la Unión (art. 3.1) y únicamente para datos relativos a servicios ofrecidos en la Unión (art. 3.3). En este sentido, no es determinante que los proveedores de servicios estén establecidos en la Unión, siendo aplicables estos instrumentos a proveedores que no estén establecidos en su territorio, si prestan servicios en la Unión; mientras que los servicios ofrecidos exclusivamente fuera de la Unión no entran en el ámbito de aplicación del Reglamento, ni aunque el proveedor de servicios esté establecido en la Unión[36].

Según la Propuesta de Reglamento, un proveedor ofrece servicios en la Unión cuando permite que personas físicas o jurídicas los utilicen en uno o más Estados miembros, siempre que también tenga una estrecha vinculación con tales Estados miembros (art. 2.4). En definitiva, no basta la mera accesibilidad del servicio, sino que es necesaria una vinculación significativa a dichos Estados[37]. Además, las órdenes europeas de entrega y conservación sólo son aplicables en el caso de que el proveedor de servicios esté establecido o representado en otro Estado miembro (y no en un contexto puramente nacional)[38], es decir, en supuestos transfronterizos, aunque la Propuesta de Reglamento no utilice este término.

---

modo un mecanismo para su aportación efectiva y eficiente al proceso a través de un sistema de gestión procesal informatizada o canales interoperables a nivel europeo". En otro caso estaríamos hablando únicamente de *datos electrónicos*, que es una modalidad concreta de prueba electrónica. Cfr. BUENO DE MATA, F., "El desafío inminente de la cooperación procesal internacional: la prueba electrónica", en *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales* (JIMÉNEZ CONDE, F., Director), Valencia, 2018, p. 274; y también, del mismo autor, "Análisis crítico de las futuras Órdenes Europeas en materia de prueba electrónica", en *La cooperación procesal internacional en la sociedad del conocimiento* (BUENO DE MATA, F., Director), Barcelona, 2019, p. 326.

36. Cfr. la explicación del art. 3 de la Exposición de Motivos y el Considerando 26.
37. Según el Considerando 28, "*debe considerarse que existe tal estrecha vinculación cuando el proveedor tenga un establecimiento en la Unión. A falta de tal establecimiento, el criterio de la estrecha vinculación debe evaluarse sobre la base de la existencia de un número significativo de usuarios en uno o más Estados miembros, o la orientación de las actividades hacia uno o más Estados miembros. La orientación hacia uno o más Estados miembros puede determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de una lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar bienes o servicios. La orientación de las actividades hacia un Estado miembro también puede derivarse de la disponibilidad de una aplicación para móvil en la tienda de aplicaciones nacional, de la publicidad local o la publicidad en la lengua utilizada en dicho Estado miembro, o de la gestión de las relaciones con los clientes, como la prestación de servicios a los clientes en la lengua comúnmente utilizada en tal Estado miembro. También se supone una estrecha vinculación cuando un proveedor de servicios dirige su actividad hacia uno o varios Estados miembros con arreglo a lo establecido en el artículo 17, apartado 1, letra c), del Reglamento n.º 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Por otra parte, la prestación de servicios con vistas a la mera observancia de la prohibición de discriminación establecida en el Reglamento (UE) 2018/302 no puede, por este único motivo, considerarse que dirige u orienta las actividades hacia un territorio determinado de la Unión*".
38. Cfr. el Considerando 15.

Entran dentro de la categoría de proveedores de servicios, las personas físicas o jurídicas que presten servicios de alguna de las siguientes clases (art. 2.3): *a)* servicios de las comunicaciones electrónicas[39]; *b)* servicios de la sociedad de la información, según se definen en el art. 1.1.b) de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, 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; y que cuenten con el almacenamiento de datos como componente esencial del servicio, en particular, las redes sociales, los mercados en línea que faciliten transacciones entre sus usuarios y otros servicios de alojamiento de datos[40]; *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[41].

En cuanto a las categorías de datos almacenados que pueden solicitarse a través de las órdenes europeas de entrega y conservación, el art. 2 distingue entre: *a) datos de los abonados*: cualquier dato relacionado con la identidad del abonado o cliente (como nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, teléfono y dirección de correo electrónico); y el tipo de servicio y su duración (incluidos los datos técnicos que identifiquen las medidas técnicas correspondientes o las interfaces, y los datos relativos a la validación del uso del servicio, excluyendo las contraseñas) (art. 2.7); *b) datos relativos al acceso*: los relativos al inicio y final de una sesión de acceso del usuario a un servicio, que sean estrictamente necesarios con el único fin de identificar al usuario del servicio, tales como la fecha y hora del acceso, o de conexión y de desconexión al servicio, junto con la dirección IP asignada al usuario, los datos identificativos de la interfaz y la identificación del usuario (art. 2.8); *c) datos de transacciones*: datos sobre transacciones relacionadas con la prestación de un servicio ofrecido por un proveedor que sirvan para facilitar

39. "*Los servicios de las comunicaciones electrónicas se definen en la Propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas. Aquí se incluyen las comunicaciones interpersonales tales como los servicios de voz sobre IP, los servicios de mensajería instantánea y los servicios de correo electrónico*" (Considerando 16).

40. Se incluyen estos otros servicios de alojamiento de datos, "*incluso en los casos en que el servicio se presta a través de la computación en la nube. Los servicios de la sociedad de la información que no cuentan con el almacenamiento de datos como componente esencial del servicio prestado al usuario, y para los que solo es de carácter secundario, como los servicios jurídicos, de arquitectura, de ingeniería y de contabilidad prestados en línea a distancia, deben quedar excluidos del ámbito de aplicación del presente Reglamento, aun cuando puedan corresponder a la definición de servicios de la sociedad de la información según lo establecido en la Directiva (UE) 2015/1535*" (Considerando 16).

41. "*Estos proveedores disponen de datos que revisten especial relevancia para las investigaciones penales, ya que pueden permitir la identificación de una persona física o jurídica responsable de un sitio web utilizado en actividades delictivas, o la identificación de la víctima de la actividad delictiva en el caso de un sitio web comprometido que haya sido secuestrado por delincuentes*" (Considerando 18).

información contextual o adicional sobre dicho servicio y sean generados y tratados por un sistema de información del proveedor, tales como el origen y destino de un mensaje u otro tipo de interacción, la ubicación del dispositivo, la fecha y hora, duración, tamaño, ruta, formato, protocolo utilizado y el tipo de compresión, a menos que estos datos constituyan datos relativos al acceso (art. 2.9); *d) datos de contenido*: todo dato almacenado en formato digital, como texto, voz, vídeos, imágenes y sonidos, distintos de los datos de los abonados, datos relativos al acceso y datos de transacciones (art. 2.10).

La propuesta de Reglamento sólo regula la obtención de datos almacenados, esto es, la obtención de datos que obren en poder del proveedor cuando reciba una orden europea de entrega o de conservación. Pero no establece una obligación general de conservación de los datos, ni permite la interceptación de datos o la obtención de datos futuros[42].

Todas estas categorías de datos contienen datos personales y están cubiertas por las garantías establecidas en el acervo de la Unión sobre protección de datos[43], aunque la intensidad de su impacto sobre los derechos fundamentales varía en cada categoría, debiendo distinguirse entre los datos de los abonados y los relativos al acceso, por una parte, en los que la afectación es menor; y los datos de transacciones y de contenido, en los que la afectación a los derechos fundamentales es mayor. Así, 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 relevante como material probatorio. De ahí que las condiciones y requisitos para obtener los datos del segundo grupo sean distintos y más rigurosos que en el caso de los primeros[44].

La clasificación entre datos de los abonados, datos de transacciones y datos de contenido era ya conocida en los ordenamientos de numerosos Estados miembros. Los datos relativos al acceso son una nueva categoría de datos

42. Cfr. el Considerando 19.
43. Junto a esta perspectiva general garantista, que es la primera que se desarrolla en el ámbito del Derecho Europeo en materia de protección de datos personales, coexiste otra vertiente del Derecho Europeo, desde la perspectiva del llamado principio de disponibilidad de los datos personales, que incide en la recogida de datos y su tratamiento en orden a la investigación y el enjuiciamiento de la criminalidad transfronteriza. Sobre esta segunda vertiente, puede verse GONZÁLEZ CANO, M.ª I., "Reflexiones sobre libre circulación de datos personales y principio de disponibilidad en el ámbito de la cooperación judicial penal en la Unión Europea", en *Derecho y Proceso. Liber Amicorum del Profesor Francisco Ramos Méndez* (CACHÓN CADENAS, M. y FRANCO ARIAS, J., Coordinadores), Barcelona, 2018, vol. II, pp. 1073 y ss.; y también, de la misma autora, "Cesión y tratamiento de datos personales en el proceso penal: aproximación a la configuración del principio de disponibilidad en el derecho de la Unión Europea", en *La cooperación procesal internacional en la sociedad del conocimiento* (BUENO DE MATA, F., Director), Barcelona, 2019, pp. 351 y ss.
44. Cfr. el Considerando 23.

introducida por la Propuesta de Reglamento, que debe asimilarse a la de datos de los abonados, ya que su finalidad es similar. En efecto, a diferencia de los datos de transacciones, que suelen buscarse para obtener información sobre los contactos y el paradero del usuario y pueden servir para establecer el perfil de un individuo, los datos relativos al acceso no sirven por sí solos para una finalidad similar, porque no revelan ninguna información sobre los interlocutores relacionados con el usuario[45].

2. AUTORIDADES EMISORAS, CONDICIONES DE EMISIÓN Y CERTIFICADOS DE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN

Las diferencias de régimen entre las distintas clases de datos almacenados están presentes en la regulación de las autoridades emisoras y de las condiciones para la emisión de las ordenes europeas de entrega y conservación. En cuanto a las autoridades emisoras, el art. 4 establece que las órdenes europeas de entrega relativa a datos de los abonados y datos relativos al acceso, así como las órdenes europeas de conservación, podrán ser emitidas por un juez, tribunal, juez de instrucción o fiscal competente; o por cualquier otra autoridad competente que actúe como autoridad de investigación en procesos penales y que tenga competencia para ordenar la obtención de pruebas, aunque en este caso la orden europea de entrega debe ser validada por alguna de las autoridades judiciales anteriormente señaladas (teniendo en cuenta que el concepto europeo de autoridad judicial incluye a los fiscales). En cambio, los fiscales no tienen competencia para emitir o validar una orden europea de entrega relativa a datos de transacciones o datos de contenido[46].

Además, conforme al art. 5, la emisión de una orden europea de entrega con respecto a datos de transacciones o datos de contenido[47] está sometida a requisitos más rigurosos que cuando se soliciten datos de los abonados o datos relativos al acceso. Así, siempre que se cumplan los requisitos generales (necesidad y proporcionalidad de la medida solicitada y previsión de una medida similar para la misma infracción penal en el ordenamiento nacional), los datos de los abonados y los relativos al acceso pueden solicitarse en la investigación de cualquier infracción penal. Mientras que sólo puede emitirse una orden europea de entrega relativa a datos de transacciones o de contenido con respecto

45. Cfr. los Considerandos 20 a 23.
46. En su Dictamen sobre la Propuesta de Reglamento, el Comité Económico y Social Europeo no considera adecuado que los fiscales puedan emitir ordenes europeas de entrega en ningún caso, entendiendo preferible que la obtención de datos de carácter personal se someta siempre a la autorización de un juez (DOUE C 367, de 10 de octubre de 2018, p. 88).
47. En este punto, la versión española contiene un error en el art. 5.4, puesto que aplica requisitos más rigurosos a la entrega de datos de transacciones o de "*datos relativos al acceso*". El error se comprueba fácilmente acudiendo a los Considerandos 31 y 32 y a la explicación del art. 5 de la Exposición de Motivos.

a: *a)* infracciones penales punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años; *b)* las infracciones penales, cometidas total o parcialmente por medio de un sistema de información, definidas en los arts. 3 a 5 de la Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; los arts. 3 a 7 de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil; y los arts. 3 a 8 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; *c)* las infracciones penales definidas en los arts. 3 a 12 y 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo.

Por su parte, según el art. 6, una orden europea de conservación podrá emitirse cuando sea necesaria y proporcionada para impedir la retirada, supresión o alteración de datos con vistas a una posterior solicitud de entrega de esos datos a través de la asistencia judicial mutua, una OEI o una orden europea de entrega, pudiendo emitirse con respecto a cualquier infracción penal.

Como puede apreciarse, se condiciona, con carácter general, la entrega de datos de transacciones y de contenido a un umbral de gravedad del delito investigado que es proporcionado, pues circunscribe dicha entrega a casos de investigación de delitos de determinada gravedad, pero sin restringirlos excesivamente, y utilizando un criterio que es fácilmente aplicable en la práctica[48]. Sin aplicar el umbral de pena, también es posible la solicitud de datos de transacciones y de contenido para la investigación de determinadas infracciones en las que las pruebas están normalmente disponibles sólo en formato electrónico, que por su naturaleza es especialmente volátil. Tampoco es aplicable el umbral de pena para la investigación de los delitos relacionados con el terrorismo[49].

La previsión de autoridades y requisitos distintos para la emisión de ordenes europeas de entrega y conservación puede dar lugar a problemas, ya que es posible que los datos conservados no puedan luego ser entregados si son datos de transacciones o de contenido.

En efecto, mientras que cualquier autoridad judicial competente, incluyendo al fiscal, puede emitir o validar una orden de conservación o una orden de entrega relativa a datos de los abonados y datos relativos al acceso, las órdenes

48. Por su parte, en su Dictamen sobre la Propuesta de Reglamento, el Comité Económico y Social Europeo ha considerado que el objetivo de que la orden europea de entrega sólo sea aplicable para formas graves de delitos, se lograría mejor mediante un umbral mínimo de pena de tres meses que mediante un umbral máximo de tres años (DOUE C 367, de 10 de octubre de 2018, p. 88).
49. Cfr. los Considerandos 31 y 32 y la explicación del art. 5 de la Exposición de Motivos.

de entrega referidas a datos de transacciones y datos de contenido sólo pueden ser emitidas o validadas por una autoridad judicial en sentido estricto, por lo tanto, con exclusión de los fiscales. De modo que puede suceder que el fiscal emita la orden europea de conservación, pero no sea competente para emitir la subsiguiente orden europea de entrega, si ésta viene referida a datos de transacciones o de contenido. Y de manera similar, como la emisión de las órdenes de entrega relativa a estos datos de transacciones y de contenido está sometida a una serie de requisitos específicos (así, un umbral de gravedad delictiva, o la investigación de determinados delitos cometidos por medio de un sistema de información o bien delitos de terrorismo) puede suceder también que, emitida una orden europea de conservación por un fiscal o incluso por una autoridad judicial en sentido estricto, sin embargo, posteriormente no sea posible solicitarlos por medio de una orden europea de entrega, si no se cumplen tales requisitos.

Por todo ello, parece que lo más lógico sería asimilar las autoridades emisoras y los requisitos según se trate de obtener o conservar datos de los abonados y datos relativos al acceso, de un lado; y datos de transacciones y datos de contenido, de otro. Por tanto, resulta preferible una regulación que no establezca distinciones entre órdenes de entrega y de conservación, a estos efectos.

Los arts. 5.5 y 6.3 establecen la información que deben incluir las órdenes europeas de entrega y conservación: *a)* la autoridad emisora y, cuando proceda, la autoridad validadora; *b)* el destinatario de la orden; *c)* las personas cuyos datos se solicitan para su entrega o conservación, excepto cuando la única finalidad de la orden sea identificar a una persona; *d)* la categoría de los datos que se solicitan para su entrega o conservación (datos de los abonados, datos relativos al acceso, datos de transacciones o datos de contenido); *e)* en su caso, el periodo que abarca la solicitud de entrega o conservación; *f)* las disposiciones de Derecho penal aplicables en el Estado emisor; *g)* la justificación de la necesidad y proporcionalidad de la medida.

Este es el contenido común a las órdenes europeas de entrega y conservación. Además, el art. 5.5 exige a las órdenes de entrega que, en caso urgente o de petición de revelación rápida de la información, incluyan las razones que lo justifiquen. Mención especial merece el último tipo de información que puede contener una orden europea de entrega. En los casos en que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa u otra entidad distinta de una persona física, conforme al art. 5.6, la orden europea de entrega sólo puede remitirse al proveedor de servicios cuando no sean apropiadas medidas de investigación remitidas a la empresa o la entidad porque podrían poner en peligro la investigación[50]. Bien, pues en estos casos, la orden de entrega debe

50. Aunque esta previsión no afecta al derecho a ordenar al proveedor de servicios que conserve los datos. Cfr. el Considerando 34.

contener la confirmación de que se solicita al amparo de esta previsión (art. 5.5)[51].

Las órdenes europeas de entrega y conservación deben remitirse directamente al representante legal designado por el proveedor de servicios a efectos de recabar pruebas para procesos penales, y si no se ha designado un representante legal específico, pueden remitirse a cualquier establecimiento del proveedor en la Unión (art. 7)[52]. Conforme al art. 8, la transmisión se realiza por medio de un certificado de orden europea de entrega, contenido en el anexo I del Reglamento e identificado en la propia Propuesta como EPOC[53]; o de un certificado de orden europea de conservación, contenido en el anexo II del Reglamento e identificado en la propia Propuesta como EPOC-PR[54]. Tanto el EPOC como el EPOC-PR deben contener toda la información exigida para la emisión de las órdenes europeas de entrega y conservación[55], respectivamente, salvo la justificación de la necesidad y la proporcionalidad de la medida u otras precisiones adicionales sobre la investigación, que no deben incluirse[56]; y en caso necesario, se traducirán a la lengua oficial de la Unión aceptada por el destinatario.

En cuanto a la forma de transmisión de los certificados de una orden europea de entrega o de una orden europea de conservación, el propio art. 8

---

51. Al respecto, aclara la explicación del art. 5 de la Exposición de Motivos: "*En los casos en que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa, normalmente en el caso de servicios de alojamiento o de programas informáticos, la propia empresa deberá ser la principal destinataria de una solicitud de las autoridades de investigación. En caso de que la empresa no sea un proveedor de servicios cubierto por el ámbito de aplicación del presente Reglamento, puede ser necesario recurrir a una orden europea de investigación o una petición de asistencia judicial. Al proveedor de servicios sólo podrá notificársele una orden europea de entrega si no procede dirigirse a la empresa, en particular cuando ello pudiera poner en peligro la investigación, por ejemplo, cuando la propia empresa esté siendo investigada*".
52. En una Nota de la Presidencia al Consejo, de 4 de octubre de 2018 (relativa a la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación, documento 12856/18), la Presidencia informa de que diversos Estados miembros han propuesto que las órdenes se notifiquen también a las autoridades judiciales del Estado miembro del destinatario o bien a las del Estado miembro de la persona cuyos datos se solicitan, de modo que también éstas pudieran evaluar la legalidad de las órdenes y cualquier posible obstáculo para su ejecución, y tendrían la posibilidad de presentar objeciones a la ejecución, aunque no hay consenso sobre a qué Estado miembro habría que enviar esta notificación, si al de ejecución o al de la persona afectada. Por su parte, la Presidencia propone como solución transaccional la notificación, únicamente a efectos informativos, a las autoridades del Estado miembro de ejecución o del Estado miembro de la persona afectada. De este modo, "*la autoridad notificada puede iniciar una consulta al Estado miembro de emisión, pero no tiene derecho a presentar objeciones a la ejecución de la orden*".
53. Por sus siglas en inglés: *European Production Order Certificate*.
54. Por sus siglas en inglés: *European Preservation Order Certificate*.
55. Incluyendo datos suficientes que permitan al destinatario identificar y ponerse en contacto con la autoridad emisora.
56. Para no poner en peligro la investigación, aunque el sospechoso podrá conocerlas e impugnarlas posteriormente durante el proceso penal. Cfr. el Considerando 38.

señala que se transmitirán directamente por cualquier medio que pueda dejar constancia escrita y permita al destinatario determinar su autenticidad[57]. En caso de que los proveedores de servicios, los Estados miembros o los organismos de la Unión hayan establecido plataformas especializadas u otros canales seguros para la tramitación de las solicitudes de datos por las autoridades policiales o judiciales, la autoridad emisora también puede transmitir el certificado por estos medios[58].

3. CUMPLIMIENTO DE LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN POR LOS PROVEEDORES DE SERVICIOS

Los arts. 9 y 10 regulan, respectivamente, la ejecución del EPOC y del EPOC-PR. No obstante, no se trata de una ejecución en sentido propio, sino del cumplimiento de los mismos por parte del destinatario, es decir, el representante legal designado por el proveedor de servicios. El procedimiento de ejecución en sentido propio se regula en el art. 14 y se atribuye a la autoridad competente del Estado de ejecución (el Estado miembro en el que resida o tenga su sede el destinatario) para el supuesto de que destinatario no haya cumplido un EPOC o un EPOC-PR.

En cuanto al cumplimiento del EPOC (art. 9), se establecen plazos breves para que el destinatario transmita directamente los datos solicitados a la autoridad emisora: diez días desde su recepción, salvo que la autoridad emisora haya indicado razones para una entrega más rápida[59]; y sin demora en los casos urgentes[60], a más tardar en un plazo de seis horas (art. 9.1 y 2). El anexo III de la Propuesta de Reglamento contiene un formulario para que el destinatario del EPOC comunique, sin demora indebida, a la autoridad emi-

57. Como el correo certificado, correo electrónico seguro, plataformas u otras vías seguras, incluidas las puestas a disposición por el proveedor de servicios, aunque éstas deberán permitir la presentación del EPOC y del EPOC-PR en el formato establecido en los anexos I y II, sin solicitar datos adicionales relativos a la orden. Cfr. el Considerando 39 y la explicación del art. 8 de la Exposición de Motivos.
58. Señala la explicación del art. 8 de la Exposición de Motivos que "*debe considerarse una posible ampliación de las plataformas eCodex y SIRIUS para incluir una conexión segura a los proveedores de servicios a efectos de la notificación del EPOC y del EPOC-PR, y en su caso, para la transmisión de las respuestas de los proveedores de servicios*".
59. "*Además del peligro inminente de supresión de los datos solicitados, tales motivos podrían incluir circunstancias relacionadas con una investigación en curso, por ejemplo, cuando los datos solicitados estén asociados a otras medidas de investigación urgentes que no puedan realizarse sin los datos en cuestión o que dependan de ellos de otro modo*" (Considerando 40).
60. Conforme al art. 2.15 de la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación, por casos urgentes deben entenderse las situaciones en las que exista una amenaza inminente para la vida o la integridad física de una persona o para una infraestructura esencial, entendida esta última tal y como se define en el art. 2.a) de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

sora las circunstancias que le impiden su cumplimiento, que pueden ser de distintos tipos.

Así, puede, en primer lugar, que el destinatario deba recurrir a dicho formulario para comunicar a la autoridad emisora que el EPOC está incompleto, contiene errores manifiestos o no contiene suficiente información para poder cumplirlo, solicitando las aclaraciones pertinentes, debiendo responder la autoridad emisora sin demora y, en todo caso, en un plazo máximo de cinco días (art. 9.3). En segundo lugar, puede que tenga que utilizarlo para informar a la autoridad emisora que no puede cumplir la orden europea de entrega por causas de fuerza mayor o imposibilidad material no imputable al destinatario o al proveedor de servicios, en particular, cuando la persona cuyos datos se solicitan no sea cliente suyo o cuando los datos se hayan suprimido antes de recibir el EPOC, lo que dará lugar, una vez comprobados los motivos, a que la autoridad emisora retire la orden (art. 9.4)[61]. Además, el destinatario también utilizará el formulario del anexo III en todos los casos en los que, por otros motivos, no aporte la información solicitada o no la facilite de forma exhaustiva o en el plazo establecido, pudiendo la autoridad emisora fijar un nuevo plazo al proveedor para la entrega de los datos (art. 9.5).

En este último supuesto, cuando el destinatario considere que el EPOC no puede ejecutarse por ser claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea o manifiestamente abusivo, también debe enviar el formulario del anexo III a la autoridad de ejecución competente de su propio Estado miembro (Estado de ejecución), quien podrá solicitar aclaraciones a la autoridad emisora, directamente o a través de Eurojust o la Red Judicial Europea. Es decir, cuando de entre esos otros motivos, la causa concreta sea la contradicción clara de la orden europea de entrega con la Carta de los Derechos de la Unión Europea o su manifiesta abusividad, el formulario del anexo III se enviará a la autoridad emisora, que puede fijar un nuevo plazo de entrega, pero también a la autoridad de ejecución, que puede pedir aclaraciones a la autoridad emisora (art. 9.5).

Cuando no entregue inmediatamente los datos solicitados, cualquiera que sea el motivo, y para garantizar su disponibilidad, el destinatario deberá conservarlos hasta su entrega, siempre que pueda identificar los datos requeridos, debiendo en caso contrario solicitar a la autoridad emisora las aclaraciones necesarias. No obstante, cuando la entrega y conservación ya no sean necesarias, la autoridad emisora deberá informar al destinatario sin demora (art. 9.6).

---

61. La comunicación a la autoridad emisora en estos casos permite que ésta pueda reaccionar con rapidez, solicitando las pruebas electrónicas a otro proveedor, y evita que se inicie un procedimiento de ejecución en supuestos en que no tiene sentido. Cfr. la explicación del art. 9 de la Exposición de Motivos.

En cuanto al cumplimiento del EPOC-PR (art. 10), el destinatario debe conservar, sin demora injustificada, los datos solicitados durante sesenta días, salvo cuando la autoridad emisora confirme que ha puesto en marcha la subsiguiente solicitud de entrega, en cuyo caso el destinatario deberá conservarlos hasta su entrega. De la misma manera que con el EPOC, la autoridad emisora informará sin demora al destinatario cuando la conservación ya no sea necesaria.

El destinatario también debe utilizar el formulario del anexo III para informar, sin demora indebida, a la autoridad emisora que no puede cumplir el EPOC-PR por las mismas causas que para el EPOC (certificado incompleto, con errores manifiestos o que no contenga información suficiente para ejecutarlo; fuerza mayor o imposibilidad material; y otros motivos) y con las mismas consecuencias, en su caso. Sin embargo, dentro de la tercera causa, que engloba, con carácter general, "*otros motivos* ", no se hace mención específica a la clara contradicción de la orden europea de conservación con la Carta de los Derechos Fundamentales de la Unión Europea o su manifiesta abusividad, como sí se contempla con respecto a la orden europea de entrega. En cualquier caso, el formulario del anexo III aplica esta concreta causa tanto al EPOC como al EPOC-PR, pero con respecto a este último, el art. 10 sólo prevé la comunicación del formulario a la autoridad emisora, pero no a la autoridad de ejecución, como en el supuesto del EPOC.

Conforme al art. 11, el destinatario debe garantizar la confidencialidad del EPOC o del EPOC-PR y, cuando se lo solicite la autoridad emisora, se abstendrá de informar a la persona cuyos datos se solicitan, con el fin de salvaguardar la investigación penal, pudiendo la propia autoridad emisora aplazar la necesaria comunicación a la persona afectada sobre la entrega de los datos durante el tiempo necesario y proporcionado[62].

Los proveedores de servicios podrán reclamar el rembolso de los gastos al Estado emisor, siempre que se contemple en la legislación nacional de éste con respecto a situaciones similares (art. 12). Finalmente, para garantizar el cumplimiento de las órdenes europeas de entrega y conservación, los Estados miembros deben establecer normas que prevean sanciones pecuniarias, tanto en casos de incumplimiento de las órdenes como del deber de confidencialidad (art. 13).

4. TRÁMITE DE RECONOCIMIENTO Y EJECUCIÓN POR LA AUTORIDAD COMPETENTE DEL ESTADO DE EJECUCIÓN, Y MOTIVOS DE DENEGACIÓN

El art. 14 regula el procedimiento de ejecución, aplicable a los casos de incumplimiento por parte del destinatario. Como hemos señalado, los desti-

62. La exigencia de comunicación a la persona afectada no se aplica a la orden europea de conservación, dada su menor injerencia en los derechos afectados (cfr. la explicación del art. 11 de la Exposición de Motivos), lo cual es coherente con la regulación del derecho al recurso del art. 17, aplicable sólo a la orden europea de entrega.

natarios de las órdenes europeas de entrega y conservación y obligados a su cumplimiento son los propios proveedores de servicios, quedando reservada la ejecución por la autoridad competente del Estado de ejecución a los supuestos de incumplimiento, a instancia de la autoridad emisora.

En realidad, el art. 14 prevé un trámite de reconocimiento y ejecución por parte de la autoridad competente del Estado de ejecución, aplicable a los supuestos de incumplimiento por parte de los destinatarios, cuando la autoridad emisora no considere aceptables los motivos esgrimidos por aquéllos para justificar su incumplimiento. En estos casos, la autoridad emisora trasladará la orden europea de entrega o conservación completa, incluyendo la justificación de su necesidad y proporcionalidad[63], junto al respectivo certificado, así como el formulario del anexo III cumplimentado por el destinatario (haciendo constar los motivos del incumplimiento) y cualquier otro documento pertinente[64], a la autoridad competente del Estado de ejecución, la cual deberá decidir sobre su reconocimiento y ejecución en el plazo máximo de cinco días hábiles (art. 14. 1 y 2). No obstante, antes denegar el reconocimiento y la ejecución, la autoridad de ejecución debe consultar a la autoridad emisora, en cuyo caso parece que no podrá cumplirse con el plazo general de 5 días hábiles establecido como plazo máximo para decidir (art. 14.7).

La autoridad de ejecución reconocerá, sin más trámites, la orden europea de entrega o la orden europea de conservación y procederá a su ejecución de conformidad a su legislación nacional, salvo que concurra alguno de los motivos de denegación enumerados en el propio art. 14. Conforme al art. 14.3, una vez que haya reconocido la orden, la autoridad de ejecución requerirá formalmente al destinatario para que, en el plazo que la propia autoridad determine, el destinatario proceda al cumplimiento o presente oposición, alegando alguna de las causas del art. 14, apartados 4 y 5. Si el destinatario presenta oposición, la autoridad de ejecución decidirá si ejecuta o no la orden, teniendo en cuenta la información facilitada por el destinatario y también la información adicional que, como ya hemos señalado, aquélla habrá debido solicitar a la autoridad emisora (art. 14.6).

Los motivos de denegación están tasados, e incluyen los motivos de oposición de los apartados 4 y 5 del art. 14, que pueden alegar los proveedores de servicios, pero que también son motivos de denegación que puede apreciar de oficio la autoridad de ejecución; más otros dos, que contempla el apartado 2 del art. 14, apreciables únicamente de oficio por la propia autoridad de ejecución.

Los apartados 4 y 5 del art. 14 enumeran las siguientes causas de denegación, aplicables tanto a la orden europea de entrega como a la de conservación:

63. Cfr. el Considerando 44.
64. Debidamente traducidos a una de las lenguas oficiales del Estado de ejecución.

1) la orden no ha sido emitida o validada por una autoridad emisora válida; *2)* el destinatario no ha podido cumplir la orden por imposibilidad material o fuerza mayor, o porque el certificado contiene errores manifiestos; *3)* la orden no se refiere a datos almacenados por el proveedor de servicios, o en su nombre, en el momento de su recepción; *4)* el servicio no está cubierto por el Reglamento; *5)* la orden es claramente contraria a las Carta de Derechos Fundamentales de la Unión Europea o manifiestamente abusiva.

Además, el apartado 4 del art. 14 incluye un motivo de denegación adicional, que sólo es aplicable a la orden europea de entrega: que, solicitándose datos de transacciones y de contenido, la infracción penal no sea de las que permiten la entrega de este tipo de datos. En cambio, la ausencia de necesidad y proporcionalidad de la orden (arts. 5.2 y 6.2), y la falta de legalidad de la misma (previsión de una medida similar para la misma infracción penal en una situación nacional comparable: art. 5.2) sólo pueden combatirse por medio de recurso en el Estado emisor, posibilidad que el art. 17 de la Propuesta de Reglamento sólo contempla con respecto a las órdenes europeas de entrega.

Como hemos dicho, estos motivos pueden ser apreciados de oficio por la autoridad de ejecución y alegados como causa de oposición por los proveedores de servicios. Además, coinciden en gran parte con los que los proveedores de servicios pueden alegar para justificar su incumplimiento, conforme a los arts. 9 y 10, pudiendo entenderse que los no contemplados expresamente en estos preceptos entrarían dentro de la categoría "*otros motivos* " (arts. 9.5 y 10.6). No obstante, sería deseable que los arts. 9, 10 y 14 coincidieran exactamente en cuanto a los motivos que los proveedores de servicios pueden oponer al cumplimiento y la ejecución de las órdenes europea de entrega y conservación[65].

Junto a los motivos del art. 14.4 y 5, el art. 14.2 incluye otras dos causas de denegación del reconocimiento y la ejecución, que sólo puede apreciar de oficio la propia autoridad de ejecución: que los datos solicitados estén protegidos por privilegios o inmunidades con arreglo a la legislación del Estado de ejecución; y que su revelación pueda afectar a los intereses nacionales del Estado de ejecución, como la seguridad y la defensa nacionales.

Las decisiones, positivas o negativas, sobre el reconocimiento y la ejecución se notificarán inmediatamente a la autoridad emisora y al destinatario

65. Aunque la técnica legislativa sea defectuosa, en el sistema de la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación, los motivos que pueden alegar los proveedores de servicios ante la autoridad emisora para justificar su incumplimiento, conforme a los arts. 9 y 10, y los que pueden esgrimir como motivos de oposición frente a la autoridad de ejecución, según el art. 14, son los mismos, lo cual se comprueba acudiendo al formulario del anexo III, Sección D, que recoge los motivos de oposición al cumplimiento de los arts. 9 y 10, haciéndolos coincidir con los de oposición a la ejecución del art. 14.

(art. 14.8). Y la autoridad de ejecución transmitirá a la autoridad emisora los datos obtenidos en el plazo de dos días hábiles (art. 14.9). Se contempla la posibilidad de que la autoridad de ejecución imponga sanciones pecuniarias, de conformidad a su legislación nacional, en el caso de que el proveedor de servicios no cumpla una orden cuya aplicabilidad haya sido reconocida por la autoridad de ejecución, previsión que viene a concretar la del art. 13 (art. 14.10).

Como conclusión común en cuanto a la regulación del cumplimiento y ejecución de la Propuesta de Reglamento, entendemos que el régimen de incidencias previsto es excesivamente amplio, con distintas posibilidades de oposición al cumplimiento en sentido propio y a la ejecución; y con diversidad de incidentes sustanciados con las autoridades de emisión y las de ejecución. Téngase en cuenta que los proveedores de servicios pueden oponerse tanto al cumplimiento como a la ejecución de las órdenes europeas de entrega y conservación, fundándose precisamente en las mismas causas, además de la potestad de la autoridad de ejecución de denegar, de oficio, el reconocimiento y la ejecución por esas mismas causas y otras adicionales. Por otra parte, los procedimientos de reexamen de las órdenes europeas de entrega, que se analizan a continuación, no son sino incidentes de oposición basados en el conflicto de la orden con la legislación de un tercer país, supuestos en los que pueden entrar en juego incluso autoridades de los países terceros. Dada su complejidad, sería deseable la simplificación de este régimen de posibles incidencias.

Aunque no se regulan en sede del trámite de ejecución de las órdenes europeas de entrega y conservación, debemos hacer referencia en último lugar en este apartado a determinadas cautelas que los arts. 5.7 y 18 establecen en relación con las órdenes europeas de entrega, sobre datos de transacciones o de contenido[66], con la finalidad de respetar los intereses del Estado miembro de ejecución. En concreto, se trata de supuestos en que los datos estén protegidos por privilegios o inmunidades concedidos por la legislación del Estado miembro del proveedor de servicios o que su revelación pueda afectar a intereses fundamentales de dicho Estado, como la seguridad y la defensa nacionales. Estos motivos coinciden con las causas de denegación del reconocimiento y la ejecución que sólo pueden ser apreciadas de oficio por la autoridad competente del Estado de ejecución, y de ahí que tratemos las mencionadas cautelas en este lugar, que, por proximidad conceptual, nos parece el más adecuado.

Así, conforme al art. 5.7, cuando la autoridad emisora entienda que los datos de transacciones o los datos de contenido *solicitados* (más bien, que

66. Los arts. 5.7 y 18 se refieren a los privilegios o inmunidades que pueden afectar a los datos de transacciones o de contenido solicitados u obtenidos a través de una orden europea de entrega. Por ello entendemos que se trata de un error, cuando el art. 5.7 incluye en su parte final los datos relativos al acceso, junto a los datos de transacciones o de contenido solicitados.

pretende solicitar) a través de una orden europea de entrega pueden estar protegidos por privilegios o inmunidades concedidos en virtud de la legislación del Estado miembro del destinatario, o afecten a intereses fundamentales de dicho Estado miembro, como la seguridad y la defensa nacionales, esta autoridad deberá pedir aclaraciones (incluso mediante consulta a las autoridades competentes del Estado miembro del destinatario, directamente o a través de Eurojust o la Red Judicial Europea en materia penal) antes de emitir la orden, y si considera que, en efecto, los datos solicitados están protegidos por privilegios e inmunidades, o que su revelación afectaría a intereses fundamentales del Estado miembro de ejecución, no emitirá la orden europea de entrega.

Por su parte, atendiendo al art. 18, cuando los datos de transacciones o los datos de contenido *obtenidos* por medio de una orden europea de entrega estén protegidos por los referidos privilegios e inmunidades previstos por la legislación del Estado miembro del destinatario o afecten a los mencionados intereses fundamentales de dicho Estado miembro, el órgano jurisdiccional del Estado emisor garantizará que durante el proceso penal respectivo esos motivos sean tenidos en cuenta en las mismas condiciones que si estuvieran previstos por su legislación nacional, al evaluar la pertinencia y la admisibilidad de las pruebas en cuestión. A tales efectos, el órgano jurisdiccional del Estado emisor podrá consultar a las autoridades del Estado de ejecución, a la Red Judicial Europea en materia penal o a Eurojust.

5. PROCEDIMIENTOS DE REEXAMEN Y RECURSOS

Los arts. 15 y 16 prevén unos procedimientos de reexamen aplicable sólo a las ordenes europeas de entrega[67], en casos de conflicto con la legislación de un país tercero (es decir, un Estado no miembro de la Unión Europea), cuando la contradicción se base en la protección de derechos o intereses fundamentales de dicho país (art. 15); o cuando la contradicción se funde en razones de otro tipo (art. 16)[68].

67. Debido al mayor grado de injerencia en los derechos de las personas afectadas.
68. Estos procedimientos de reexamen previstos para casos de conflicto con la legislación de un país tercero activan un control judicial y son equivalentes a la *cláusula de cortesía* de la Ley estadounidense CLOUD [*U.S. Cloud Act*, *Clarifying Lawful Overseas Use of Data*, de 23 de marzo de 2018 (Ley de aclaración del uso legítimo de los datos en el extranjero)]. La cláusula de cortesía permite a los proveedores de servicios norteamericanos solicitar a un tribunal estadounidense que anule o modifique una orden emitida para la protección o divulgación de datos, si éstos se refieren a un nacional de un país distinto a los Estados Unidos y el acatamiento de la orden supone la violación de las leyes de un país con el que los Estados Unidos ha celebrado un acuerdo ejecutivo que contempla posibilidades similares para los proveedores de servicios con arreglo a sus leyes [cfr. la Nota de la Presidencia al Consejo, de 28 de mayo de 2018 (9418/18), relativa a las Propuestas de Reglamento sobre las órdenes europeas de entrega y conservación y de Directiva sobre los representantes legales para recabar pruebas para procesos penales]. Como ya hemos señalado y analizaremos posteriormente, la Unión Europea pretende alcanzar un Acuerdo

En el primer supuesto, es decir, cuando el destinatario considere que existe un conflicto entre la orden europea de entrega y la legislación del país tercero que prohíbe revelar los datos en cuestión para proteger los derechos fundamentales de los interesados o los intereses fundamentales del país relacionados con la seguridad y la defensa nacionales, notificará a la autoridad emisora su oposición motivada[69], a través del formulario del anexo III (concretamente, el art. 15.1 remite al procedimiento del art. 9.5), conteniendo la información sobre la legislación del país tercero, su aplicabilidad al caso y la naturaleza de la obligación contradictoria (art. 15.1 y 2)[70].

La autoridad emisora revisará la orden, pudiendo anularla. Pero si entiende que procede su confirmación, debe solicitar una revisión por el órgano jurisdiccional competente de su propio Estado miembro (Estado emisor), el cual evaluará si existe el conflicto, examinando si, en el caso concreto, es aplicable la legislación del país tercero y, de ser así, si la misma prohíbe la revelación de los datos solicitados (art 15.3)[71].

La autoridad jurisdiccional competente confirmará la orden cuando entienda que no existe conflicto. En caso contrario, deberá consultar a la autoridad central del país tercero, y si ésta se opone a la ejecución de la orden, el órgano jurisdiccional competente la anulará. Para evacuar este trámite de consulta a la autoridad central del país tercero, el órgano jurisdiccional competente del Estado emisor le transmitirá, a través de su propia autoridad central nacional, los elementos de hecho y de Derecho atinentes al caso, así como la evaluación realizada por el órgano jurisdiccional. Cuando la autoridad central del país tercero comunique su oposición a la ejecución de la orden europea de entrega, el órgano jurisdiccional la anulará, informando de ello tanto a la autoridad emisora como al destinatario. Si aquélla no contesta en plazo, se le enviará un recordatorio y si tampoco contesta[72], el órgano jurisdiccional

---

con los Estados Unidos de América, de manera que los proveedores de servicios estadounidenses y europeos puedan ofrecer datos directamente a las autoridades de la otra parte (los proveedores de servicios estadounidenses a las autoridades europeas, y los proveedores de servicios europeos a las autoridades estadounidenses).

69. No obstante, concreta el art. 15.2 que la oposición no podrá basarse en la ausencia, en la legislación del país tercero, de procedimientos similares a la orden europea de entrega, ni en la única circunstancia de que los datos se almacenen en un país tercero.
70. La Sección D del formulario del anexo III incluye el conflicto con la legislación de un país tercero como motivo de oposición a una orden europea de entrega, dedicándose la Sección E a las explicaciones relativas a la legislación del país tercero, su aplicabilidad al caso y la naturaleza de la obligación contradictoria.
71. El órgano jurisdiccional tendrá en cuenta si la legislación del país tercero, en lugar de proteger los derechos fundamentales o los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, pretende manifiestamente proteger otros intereses o tiene como objetivo proteger actividades ilegales frente a requerimientos policiales o judiciales en el contexto de investigaciones penales (art. 15.4).
72. El plazo para contestar es de 15 días, que pueden prorrogarse por 30 días, previa solicitud

competente confirmará la orden, informando de ello a la autoridad emisora y al destinatario, para que este último proceda a su cumplimiento (art. 15,5-7).

Cuando se trate de la contradicción con la legislación de un país tercero no destinada a proteger derechos fundamentales ni los intereses fundamentales del país (art. 16), el procedimiento se desarrolla del mismo modo, pero en este caso es el órgano jurisdiccional competente del Estado emisor el que decide en todo caso sobre la existencia o no del conflicto, confirmando o anulando la orden europea de entrega, sin consulta a la autoridad central del país tercero. Si el órgano jurisdiccional competente considera que no existe conflicto relevante confirmará la orden, y cuando compruebe que la legislación del país tercero prohíbe la revelación de los datos solicitados confirmará o retirará la orden, ponderando una serie de elementos que pretenden determinar el grado de vinculación de la causa penal en la que se ha emitido la orden con cualquiera de las dos jurisdicciones (Estado emisor o país tercero), sus respectivos intereses para obtener los datos o impedir su revelación, y las posibles consecuencias que para el proveedor de servicios conlleva el cumplimiento de la orden[73]. El órgano jurisdiccional competente informará de su decisión de anular o confirmar la orden europea de entrega, tanto a la autoridad emisora como al destinatario, quien, en su caso, deberá proceder a dar cumplimiento a la orden.

Como ambos supuestos de reexamen suspenden la ejecución de la orden europea de entrega, el destinatario debe conservar los datos durante su tramitación (por aplicación del art. 9.6), y cuando la orden se anule, puede emitirse una orden europea de conservación para garantizar la disponibilidad de los datos y permitir que la autoridad emisora los solicite por otras vías, como la asistencia judicial mutua[74].

Conforme al art. 17, aplicable también únicamente a las órdenes europeas de entrega, todas las personas afectadas deben poder impugnar la orden, tanto los sospechosos o acusados, durante el propio proceso penal en el que se haya

---

motivada de la autoridad central del país tercero. Tras el recordatorio, la autoridad central del país tercero cuenta con un plazo adicional de otros cinco días.

73. Según el art. 16.5, los elementos que debe ponderar el órgano jurisdiccional competente son los siguientes: *a)* el interés protegido por la legislación del país tercero, incluido el interés en impedir la revelación de los datos; *b)* el grado de vinculación de la causa penal en la que se haya emitido la orden con cualquiera de las dos jurisdicciones, determinado, entre otros extremos, por la ubicación, nacionalidad y lugar de residencia de la persona cuyos datos se solicitan o de la víctima; y por el lugar de comisión del delito investigado; *c)* el grado de vinculación entre el proveedor de servicios y el país tercero, sin que sea suficiente el lugar de almacenamiento de los datos para establecer un grado de vinculación significativo; *d)* los intereses del Estado investigador en obtener las pruebas reclamadas, en función de la gravedad del delito y la importancia de la obtención de pruebas con prontitud; *e)* las posibles consecuencias para el destinatario o el proveedor de servicios de cumplir la orden europea de entrega, incluidas las sanciones que puedan aplicarse.
74. Cfr. el Considerando 53 y la explicación de los arts. 15 y 16 de la Exposición de Motivos.

emitido la orden; como los que no lo son, que también deben tener vías de recurso efectivas en el Estado emisor (art. 17.1 y 2)[75]. Realmente, lo que este precepto regula es la impugnación de la incorporación de la prueba obtenida al proceso penal, pues se refiere específicamente a los *datos obtenidos*. Y por ello se establece que "*los Estados miembros velarán por que, en los procesos penales en el Estado emisor, se respeten los derechos de la defensa y la equidad del proceso al evaluar las pruebas obtenidas a través de la orden europea de entrega*" (art. 17.6).

Estos recursos se ejercitarán ante un órgano jurisdiccional del Estado emisor conforme a su legislación nacional[76], y deberán incluir en todo caso la posibilidad de impugnar la legalidad (hay que entender que se refiere a la previsión en el Estado emisor de una medida similar para la misma infracción penal en una situación nacional comparable), la necesidad y la proporcionalidad de la orden europea de entrega, requisitos exigidos por el art. 5.2 de la Propuesta de Reglamento (art. 17.3)[77]. A este respecto, la autoridad emisora velará para que se facilite información a la persona afectada sobre las posibilidades de recurso, sin perjuicio de la posibilidad de aplazar esta información en los casos del art. 11, para no comprometer el buen fin de la investigación penal (art. 17.4).

IV. LAS NEGOCIACIONES PARA UN ACUERDO ENTRE LA UNIÓN EUROPEA Y LOS ESTADOS UNIDOS DE AMÉRICA SOBRE EL ACCESO TRANSFRONTERIZO A LAS PRUEBAS PENALES ELECTRÓNICAS

Como hemos señalado, la Unión Europea pretende alcanzar un Acuerdo con los Estados Unidos sobre el acceso transfronterizo, por parte de las autoridades judiciales penales, a las pruebas de carácter electrónico que obren en poder de los proveedores de servicios. Y para ello, la Comisión Europea ha presentado la *Recomendación de Decisión del Consejo por la que se*

75. Todo ello, sin perjuicio de que tanto los sospechosos y acusados como las demás personas afectadas por la orden puedan ejercer las vías de recurso disponibles con arreglo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos (*Directiva sobre protección de datos en el ámbito penal*); y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (*Reglamento general de protección de datos*).

76. El art. 17.5 dispone que los plazos u otras condiciones para la interposición de un recurso serán iguales a los previstos en casos internos similares, lo cual ya se sobreentendía por la remisión a la legislación nacional del Estado emisor.

77. En este sentido, el Reglamento no debe limitar los posibles motivos para impugnar la orden. Cfr. el Considerando 54.

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 2019[78]. A continuación, trataremos de explicar los aspectos más relevantes de los objetivos y las directrices de negociación contenidos en este documento.

En cuanto al contexto y la situación de partida de esta propuesta, Estados Unidos es el principal receptor de solicitudes de asistencia judicial mutua emitidas desde los Estados miembros de la Unión Europea para acceder a pruebas penales electrónicas, ya que los principales proveedores de servicios operan sujetos a la jurisdicción de aquel país. Pero la cooperación judicial con Estados Unidos resulta demasiado lenta, si se tiene en cuenta el carácter volátil de las pruebas electrónicas, y puede suponer un gasto desproporcionado de recursos. Por ello, la cooperación directa con los proveedores de servicios de los Estados Unidos se ha convertido en un canal alternativo a la cooperación judicial. No obstante, aunque ofrece un acceso más rápido, la cooperación directa se limita a los datos sin contenido y, además, tiene carácter voluntario, según la legislación norteamericana. Por ello, menos de la mitad de las solicitudes efectuadas a proveedores de servicios norteamericanos reciben respuesta. En cuanto a las solicitudes recíprocas, las autoridades de los Estados Unidos, con carácter general, sólo pueden obtener las pruebas electrónicas a través de la asistencia judicial mutua, pues muchos Estados miembros de la Unión Europea prohíben a los proveedores de servicios nacionales responder directamente a solicitudes de autoridades extranjeras, incluso las que se refieren a datos sin contenido[79].

Aunque la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas penales electrónicas incluye procedimientos de revisión para el caso de que el proveedor de servicios se enfrente a obligaciones contradictorias derivadas de la legislación de un tercer país, el objetivo de un Acuerdo entre la Unión Europea y los Estados Unidos de América es evitar la existencia de obligaciones contradictorias entre ellos[80]. Este Acuerdo es posible al amparo de la Ley CLOUD estadounidense[81], que permite celebrar acuerdos ejecutivos con gobiernos extranjeros, según los cuales los proveedores de servicios norteamericanos podrían facilitar datos de contenido directamente a dichos gobiernos extranjeros.

78. COM(2019) 70 final.
79. Cfr. la Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 1: "*Contexto*".
80. Cfr. la Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 2: "*Objetivos de la Propuesta*".
81. *Clarifying Lawful Overseas Use of Data*, de 23 de marzo de 2018.

Según las directrices de negociación elaboradas por la Comisión Europea[82], el Acuerdo debe aclarar el carácter vinculante y la ejecutoriedad de las órdenes dirigidas a los proveedores de servicios y detallar las obligaciones de las autoridades judiciales. Y el objetivo del Acuerdo debe ser triple: *a)* establecer normas comunes y resolver los conflictos de leyes que puedan suscitar las órdenes sobre datos de contenido y datos sin contenido procedentes de una autoridad judicial de una Parte contratante y dirigidas a un proveedor de servicios sujeto a la legislación de otra Parte contratante; *b)* con base en dichas órdenes, permitir las transferencia de pruebas electrónicas directamente y con carácter recíproco, de un proveedor de servicios a la autoridad solicitante; *c)* velar por el respeto de los derechos y libertades fundamentales y de los principios generales del Derecho de la Unión Europea, reconocidos en los Tratados y en la Carta de Derechos Fundamentales.

Conforme a las mismas directrices, el Acuerdo entre la Unión Europea y los Estados Unidos debe ser compatible con las Propuestas europeas (Reglamento y Directiva) sobre pruebas penales electrónicas, tanto a medida que evolucionen en el procedimiento legislativo como en su versión final. Por ello, las directrices de negociación de la Comisión proponen un Acuerdo en términos similares a los de sus Propuestas de Reglamento y Directiva. Además, en el marco de las relaciones entre los Estados Unidos de América y la Unión Europea, el Acuerdo debe tener prioridad frente al Convenio sobre Ciberdelincuencia del Consejo de Europa y a cualquier acuerdo alcanzado en las negociaciones del Segundo Protocolo adicional a dicho Convenio, en la medida en que las disposiciones de estos últimos contemplen cuestiones previstas en el Acuerdo[83].

Finalmente, las directrices de negociación de la Comisión Europea contemplan una serie de garantías adicionales al Acuerdo entre la Unión Europea y los Estados Unidos en materia de protección de datos y privacidad, conocido como el *Acuerdo Marco*, que entró en vigor el 1 de febrero de 2017[84]. Estas garantías son de dos tipos. Las primeras, son garantías adicionales en materia de privacidad y protección de datos, y están referidas a los objetivos para los que pueden solicitarse y transferirse los datos personales y los datos de comunicaciones electrónicas y a los requisitos para su uso y divulgación, y su transferencia posterior. Las segundas son derechos procesales adicionales

82. Cfr. el Anexo a la Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 1: "*Objetivos*".
83. Cfr. el Anexo a la Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 1: "*Objetivos*"; y epígrafe 2: "*Naturaleza y ámbito de aplicación del Acuerdo*".
84. Cfr. el Anexo a la Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 3: "*Garantías*".

que la Comisión propone teniendo en cuenta la especialidad de los requisitos para la transferencia de pruebas electrónicas directamente por los proveedores de servicios, en lugar de entre autoridades. "*Entre esos derechos se incluye el de que los datos no puedan ser solicitados para su uso en procesos penales que pueden conducir a la pena de muerte, la proporcionalidad de las órdenes, y garantías específicas en el caso de datos protegidos por privilegios e inmunidades. Los privilegios e inmunidades de determinadas profesiones, como la de abogado, así como los intereses fundamentales de seguridad y defensa nacionales del Estado destinatario, también deberán tenerse en cuenta durante el proceso en el Estado emisor. La revisión por una autoridad judicial funciona como una garantía adicional a este respecto*[85]".

V. VALORACIÓN FINAL

Debemos felicitarnos por esta iniciativa de la Unión Europea para facilitar la obtención transfronteriza de pruebas penales electrónicas, a través de las órdenes europeas de entrega y conservación. Bueno es que contemos con instrumentos específicos, adaptados a las características especiales de las pruebas electrónicas. Ahora bien, centrándonos en la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación, es evidente que el régimen jurídico presentado por la Comisión Europea es sólo una propuesta inicial que necesita mejoras.

Ya hemos señalado que nos parece criticable la previsión de autoridades y requisitos distintos para la emisión de las órdenes de entrega y las de conservación, habiendo abogado por la asimilación de las autoridades emisoras y los requisitos según se trate de obtener o conservar datos de los abonados y datos relativos al acceso, de un lado; y datos de transacciones y datos de contenido, de otro (siempre y cuando se conserve la tajante distinción entre ambas categorías de datos). También hemos criticado la excesiva amplitud del régimen de incidencias previsto en cuanto al cumplimiento y la ejecución, con distintas posibilidades de oposición al cumplimiento en sentido propio y a la ejecución; y con diversidad de incidentes sustanciados con las autoridades de emisión y las de ejecución, e incluso con autoridades de terceros países, en el caso de los procedimientos de reexamen. Sería deseable la simplificación de este panorama de posibles incidencias.

A las críticas anteriores, añadimos ahora que también resultan discutibles otras diferencias que se establecen entre las órdenes europeas de entrega y las de conservación, basadas en la supuesta menor injerencia en los derechos de las personas afectadas de las órdenes de conservación con respecto a las de

85. Recomendación de Decisión del Consejo sobre un Acuerdo con los Estados Unidos de América sobre el acceso transfronterizo a las pruebas penales electrónicas, epígrafe 3: "*Disposiciones pertinentes en la misma política sectorial*".

entrega, y que justifican que los procedimientos de reexamen (arts. 15 y 16), las vías de recurso efectivas (art. 17) e, incluso, los privilegios e inmunidades concedidos por la legislación del Estado de ejecución (arts. 5.7 y 18) sólo se apliquen a las órdenes europeas de entrega y no a las de conservación. Esto tiene consecuencias relevantes, por ejemplo, impide que pueda impugnarse la legalidad, necesidad y proporcionalidad de una orden de conservación. Por ello, entendemos que, a salvo aspectos puntuales que justifiquen la diferencia, podría unificarse el régimen de las órdenes europeas de entrega y conservación.

Parece, incluso, necesitada de mayor reflexión la radical distinción que se establece entre las categorías de datos de los abonados y los relativos al acceso, y los datos de transacciones y de contenido, con consecuencias en cuanto a las autoridades y los requisitos de emisión, entre otros aspectos. Porque haciendo una traslación simplista de las previsiones de la Propuestas de Reglamento al ordenamiento español parecería que sólo las órdenes europeas de entrega relativas a datos de transacciones y de contenido podrían considerarse limitativas de los derechos fundamentales (de ahí que sólo puedan emitirse por una autoridad judicial en sentido estricto, y no por un fiscal, y con requisitos más rigurosos), lo cual resulta, al menos, discutible.

Pero el aspecto más problemático del nuevo sistema propuesto para la obtención transfronteriza de pruebas penales electrónicas es, precisamente, el que resulta más novedoso y sobre el que se hace recaer, en gran medida, la eficacia del sistema, esto es, que las órdenes europeas de entrega y conservación no se dirijan a una autoridad judicial del Estado de ejecución, sino directamente a los proveedores de servicios, a los que se les impone la obligación de cumplirlas (con posibilidad de imposición de sanciones pecuniarias), reservando a la autoridad competente de aquel Estado la ejecución en caso de incumplimiento. La Propuesta de la Comisión Europea caracteriza las órdenes europeas de entrega y conservación como instrumentos de reconocimiento mutuo en el ámbito de la cooperación judicial penal, pero, paradójicamente, articula un sistema, no de comunicación directa entre autoridades judiciales, sino entre una autoridad judicial y un proveedor de servicios, que es una entidad privada. Con ello, el control judicial en el Estado de ejecución será sólo eventual, en una materia que afecta de lleno a los datos personal y la privacidad y, por tanto, a los derechos fundamentales[86].

86. De instaurarse así este sistema se produciría la *privatización* del reconocimiento mutuo. Cfr. en este sentido, MITSILEGAS, V., "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence", *Maastricht Journal of European and Comparative Law*, 2018, Vol. 25(3), pp. 263-265. Véase también al respecto, STEFAN, M. y GONZÁLEZ FUSTER, G., "Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US", *CEPS Paper in Liberty and Security in Europe*, n.º 2018-07, November 2018.

Por lo demás, las pruebas electrónicas pueden ser más fáciles de manipular por lo que necesitan garantías adicionales y específicas que permitan mantener la cadena de custodia, asegurando su autenticidad e integridad durante todo el proceso de recogida, conservación, transmisión y entrega de las mismas. Tratándose de un sistema europeo de obtención transfronteriza de pruebas electrónicas sería deseable que la Unión Europea estableciese unas normas mínimas comunes al respecto (que no se contienen en la normativa propuesta por la Comisión), y que garantizarían la admisibilidad de las pruebas electrónicas en el Estado que las solicitó[87].

87. Cfr. BIASIOTTI, M.ª A., "A proposed electronic evidence exchange across the European Union", Digital Evidence and Electronic Signature Law Review, 14 (2017). También, desde un análisis general de la gestión procesal de las pruebas electrónicas, AMANN, P. y DILLON, M. P., "Electronic Evidence Management at the ICC: Legal, Technical, Investigative and Organizational Considerations", en International Criminal Investigations. Law and Practice (AA. VV.), Eleven International Publishing, 2018, pp. 231 y ss.