

## DOCTRINA



# Nuevas perspectivas para la obtención transfronteriza de prueba penal electrónica en la Unión Europea (1)

**Luis Gómez Amigo**

*Catedrático de Derecho Procesal. Universidad de Almería*

### Resumen

**En este trabajo se analizan las características esenciales de las órdenes europeas de entrega y conservación, que son los nuevos instrumentos de reconocimiento mutuo que pretende establecer la Unión Europea para la obtención transfronteriza de pruebas penales electrónicas.**

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. A menudo las redes sociales y los servicios de correo electrónico y de mensajería instantánea son el único lugar donde los investigadores pueden hallar pistas para investigar el delito y pruebas para perseguirlo. Por ello, 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, adaptada a las particularidades de esta clase de pruebas: la orden europea de entrega y la orden europea de conservación. 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. Con esta iniciativa legislativa, 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 comunicaciones electrónicas y de la sociedad de la información en la Unión que entregue o conserve pruebas electrónicas, a través de una orden europea de entrega o 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.

## I. INTRODUCCIÓN

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 importante avance 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 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) .

**La OEI supone un destacado avance frente a los anteriores**

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 2008/978/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.

## instrumentos de reconocimiento mutuo

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 se consigue configurando la OEI como una 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.

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 instantánea son el único lugar donde los investigadores pueden hallar pistas para investigar el delito y pruebas para perseguirlo. 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. 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 (6) .

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) 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 (7) , 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 comunicaciones electrónicas y de la sociedad de la información en la Unión (8) que entregue o conserve pruebas electrónicas, a través de una orden europea de entrega o 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 (9) .

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 (10) . En ella, se establece la obligación de que los proveedores de servicios (11) 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 (12) .

El objetivo de este trabajo es examinar, a grandes rasgos, esta nueva iniciativa europea para facilitar el acceso transfronterizo a las pruebas penales electrónicas, que es la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

## II. LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN DE PRUEBAS PENALES ELECTRÓNICAS: CONCEPTO, FINALIDAD Y ÁMBITO DE APLICACIÓN

Atendiendo a su objeto, definiciones y ámbito de aplicación (arts. 1-3), la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación regula las ordenes que la autoridad de un Estado miembro pueden dirigir 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).

Conforme a su ámbito de aplicación, sólo pueden dirigirse estas órdenes a proveedores que ofrezcan sus servicios en la Unión y en el ámbito de investigaciones o procesos penales sobre infracciones penales determinadas, «tanto durante las fases previas al juicio como durante la fase procesal» (art. 3.2) (13) . 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) (14) , es decir, en supuestos transfronterizos, aunque la Propuesta de Reglamento no utilice este término.

Entran dentro de la categoría de proveedores de servicios, las personas físicas o jurídicas que presten servicios de alguna de las siguientes clases (art. 2.2): a) servicios de las comunicaciones electrónicas (15) ; 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 (16) ; 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 (17) .

De entre las definiciones del art. 2, son especialmente relevantes las que hacen referencia a las categorías de datos almacenados que pueden solicitarse a través de las órdenes europeas de entrega y conservación (18) : a) *datos de los abonados*: cualquier dato relacionado con la identidad del abonado o cliente y el tipo de servicio y su duración; 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; c) *datos de transacciones*: datos sobre transacciones relacionadas con la prestación de un servicio ofrecido por un proveedor que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados y tratados por un sistema de información del proveedor; 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.

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, 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 (19) . 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 (20) .

### III. AUTORIDADES EMISORAS, CONDICIONES DE EMISIÓN Y CERTIFICADOS

Esta diferencia de régimen está presente en relación con la regulación de las autoridades emisoras y 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. 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 (21) .

Conforme al art. 5, la emisión de una orden europea de entrega con respecto a datos de



transacciones o datos de contenido (22) está sometida a requisitos más rigurosos que cuando se soliciten datos de los abonados o datos relativos al acceso. Así, además de cumplir con 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 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.

**Una orden europea de conservación podrá emitirse cuando sea necesaria y proporcional para impedir la retirada, supresión o alteración de datos**

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 (23) . 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 (24) .

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) (25) . 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 (26) ; 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 (27) . Tanto el EPOC como el EPOC-PR deben contener toda la información exigida para la emisión de las órdenes europeas de entrega y conservación, respectivamente, salvo la justificación de la necesidad y la proporcionalidad de la medida u otras precisiones adicionales sobre la investigación (28) ; se transmitirán directamente por cualquier medio que pueda dejar constancia escrita y permita al destinatario determinar su autenticidad (29) ; y en caso necesario, se traducirán a la lengua oficial de la Unión aceptada por el destinatario

(art. 8).

#### IV. CUMPLIMIENTO Y EJECUCIÓN

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 para el supuesto de que destinatario no haya cumplido un EPOC o un EPOC-PR.

Se establecen breves plazos para el cumplimiento del EPOC por el destinatario: diez días desde su recepción, salvo que la autoridad emisora haya indicado razones para una entrega más rápida (30) ; y sin demora en los casos urgentes (31) , a más tardar en un plazo de seis horas. El anexo III de la Propuesta de Reglamento contiene un formulario para que el destinatario del EPOC comunique a la autoridad emisora 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 que el EPOC está incompleto, contiene errores manifiestos o no contiene suficiente información para poder cumplirlo. En segundo lugar, puede que tenga que utilizarlo para informar a la autoridad emisora que no puede cumplir el EPOC 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 (32) . 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.

A diferencia de los supuestos anteriores, 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, debe enviar el formulario del anexo III, pero en este caso, 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.

Cuando no entregue inmediatamente los datos solicitados, cualquiera que sea el motivo, y para garantizar su disponibilidad, el destinatario deberá conservarlos, siempre que pueda identificar los datos requeridos.

En cuanto al cumplimiento del EPOC-PR, 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. El destinatario también debe utilizar el formulario del anexo III para indicar a la autoridad emisora que no puede cumplir el EPOC-PR por las mismas tres primeras causas que para el EPOC, pero no en el cuarto caso, que daba lugar a la comunicación a la autoridad de ejecución, que no se contempla para la orden de conservación.

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 (33) .

**El art. 14 regula el procedimiento de ejecución, aplicable a los casos de incumplimiento por parte del destinatario**

El art. 14 regula el procedimiento de ejecución, aplicable a los casos de incumplimiento por parte del destinatario. La autoridad emisora trasladará la orden europea de entrega o conservación completa, incluyendo la justificación de su necesidad y proporcionalidad, junto al respectivo certificado (34) , a la autoridad competente del Estado de ejecución, la cual deberá ejecutarla de conformidad a su legislación nacional. Por su parte, el destinatario puede oponerse a la ejecución en virtud de una serie de motivos tasados (35) , decidiendo finalmente la autoridad de ejecución, que también puede denegar el reconocimiento y la ejecución cuando considere que los datos en cuestión están protegidos por privilegios o inmunidades con arreglo a su legislación nacional o que su revelación puede afectar a intereses fundamentales, como la seguridad y la defensa nacionales. Antes de denegar el reconocimiento o la ejecución de una orden europea, la autoridad de ejecución debe consultar a la autoridad emisora.

## V. PROCEDIMIENTO DE REEXAMEN Y RECURSOS

Los arts. 15 y 16 prevén un procedimiento de reexamen aplicable sólo a las ordenes europeas de entrega (36) , en casos de contradicción con la legislación de un país tercero, basada en la protección de derechos o intereses fundamentales de dicho país, o cuando la contradicción se funde en razones de otro tipo. En el primer supuesto, 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, a través del formulario del anexo III. 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, quien a su vez, si entiende que puede existir el conflicto planteado, 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.

Cuando se trate de la contradicción con la legislación de un país tercero no destinada a proteger los derechos fundamentales ni los intereses fundamentales del país, 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, 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, incluidas las sanciones que puedan aplicarse (37) .



Como ambos supuestos de reexamen suspenden la ejecución de la orden europea de entrega, los datos deben conservarse durante su tramitación, 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 (38) .

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 emitido la orden; como los que no lo son, que también deben tener vías de recurso efectivas en el Estado emisor (39) . Este precepto parece limitar la impugnación a la incorporación de la prueba al proceso penal, pues se refiere específicamente a los *datos obtenidos*. Estos recursos se ejercitarán ante un órgano jurisdiccional del Estado emisor conforme a su legislación nacional, y deberán incluir en todo caso la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la orden europea de entrega (40) .

Para terminar con el examen de las características esenciales de esta Propuesta de Reglamento, se establecen determinadas cautelas en relación con las órdenes europeas de entrega, para respetar los privilegios e inmunidades establecidos en la legislación del Estado de ejecución. Así, cuando los datos de transacciones o los datos de contenido *solicitados* a través de una orden europea de entrega estén 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, la autoridad emisora deberá pedir aclaraciones (incluso mediante consulta a las autoridades competentes del Estado miembro de ejecución) antes de emitir la orden, y si considera que, en efecto, los datos solicitados (41) 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 (art. 5.7). Por su parte, 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 o afecten a los mencionados intereses fundamentales, 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 (art 18).

## VI. CONCLUSIÓN

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. Además, resulta muy adecuado que los destinatarios de las mismas y obligados a su cumplimiento sean los representantes legales de los propios proveedores de servicios, quedando reservada la ejecución por la autoridad competente del Estado de ejecución a los supuestos de incumplimiento.

No obstante, ya se advierten algunos aspectos susceptibles de mejora. Así, 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 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. Y, por tanto, sin hacer distinciones entre órdenes de entrega y de conservación, a estos efectos. Otras diferencias de régimen entre las órdenes europeas de entrega y las de conservación sí parecen razonables, pues hacen referencia a garantías que sólo entrarían en juego en caso de entrega de los datos. Así, por ejemplo, los procedimientos de reexamen de los arts. 15 y 16, o las vías de recurso efectivas del art. 17.

Además, el régimen de incidencias en cuanto al cumplimiento y la ejecución es muy amplio, con distintas posibilidades de oposición al cumplimiento en sentido propio y a la ejecución, y con diversidad de incidentes sustanciados, tanto con las autoridades de emisión como de ejecución, e incluso con autoridades de terceros países. Dada su complejidad, sería deseable la simplificación de este régimen de posibles incidencias.

Mención especial merece la previsión de la tutela de los derechos e intereses de terceros estados a través de los procedimientos de reexamen de los arts. 15 y 16. En realidad, el país tercero por excelencia es Estados Unidos, o lo que es lo mismo, se trata de disposiciones que parecen mirar fundamentalmente a dicho país. Estos procedimientos de reexamen previstos en la Propuesta de Reglamento europeo para casos de conflicto con la legislación de un país tercero son equivalentes a la *cláusula de cortesía* de la Ley estadounidense CLOUD (*U.S. Cloud Act*) (42) , cláusula de cortesía que permite a los proveedores de servicios 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. Actualmente, la Unión Europea se encuentra estudiando la conveniencia de celebrar un acuerdo ejecutivo con los Estados Unidos, 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), en las condiciones estipuladas en el acuerdo ejecutivo (43) .

(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.

[Ver Texto](#)

- (2) Conforme a los Considerandos 44 y 45, la Directiva sobre la OEI no se aplica ni a Irlanda ni a Dinamarca.

[Ver Texto](#)

- (3) Así lo dispone el art. 34 de la Directiva sobre la OEI.

[Ver Texto](#)

- (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 es parcial, pues sólo se produce en relación con el aseguramiento de pruebas. Además, el Reglamento (UE) 2016/95, de 20 de enero de 2016, ha derogado la Decisión Marco 2008/978/JAI.

[Ver Texto](#)

- (5) Así lo dispone el art. 13 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.

[Ver Texto](#)

- (6) COM (2018) 225 final.

[Ver Texto](#)

- (7) 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, que contiene también una explicación detallada de los preceptos contenidos en la Propuesta.

[Ver Texto](#)

- (8) 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.

[Ver Texto](#)

- (9) En cambio, la intervención de las telecomunicaciones sí está prevista en los arts. 30 y 31 de la Directiva sobre la OEI.

[Ver Texto](#)

- (10) COM (2018) 226 final.

[Ver Texto](#)

- (11) 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.

[Ver Texto](#)

- (12) 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

también una explicación detallada de los preceptos contenidos en la Propuesta.

Ver Texto

- (13) 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).

Ver Texto

- (14) Cfr. el Considerando 15.

Ver Texto

- (15) *«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).

Ver Texto

- (16) 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).

Ver Texto

- (17) *«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).

Ver Texto

- (18) 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. Cfr. el Considerando 19.

Ver Texto

- (19) 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 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. Cfr. los Considerandos 20 a 23.

Ver Texto

(20) Cfr. el Considerando 23.

[Ver Texto](#)

(21) 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, pág. 88).

[Ver Texto](#)

(22) 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.

[Ver Texto](#)

(23) 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, pág. 88).

[Ver Texto](#)

(24) Cfr. los Considerandos 31 y 32 y la explicación del art. 5 de la Exposición de Motivos.

[Ver Texto](#)

(25) 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, n.º doc. prec.: 12115/18), 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*».

[Ver Texto](#)

(26) Por sus siglas en inglés: *European Production Order Certificate*.

[Ver Texto](#)

(27) Por sus siglas en inglés: *European Preservation Order Certificate*.

[Ver Texto](#)

(28) Para no poner en peligro la investigación, aunque el sospechoso podrá conocerlas e impugnarlas posteriormente durante el proceso penal. Cfr. el Considerando 38.

[Ver Texto](#)

(29) 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.

Ver Texto

- (30) «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).

Ver Texto

- (31) Conforme al art. 2.14 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.

Ver Texto

- (32) 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 inicie un procedimiento de ejecución en supuestos en que no tiene sentido. Cfr. la explicación del art. 9 de la Exposición de Motivos.

Ver Texto

- (33) 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.

Ver Texto

- (34) Cfr. el Considerando 44.

Ver Texto

- (35) El art. 14.4 y 5 enumera las siguientes causas de denegación, aplicables tanto al EPOC como al EPOC-PR: 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 aquélla contiene errores manifiestos; 3) la orden no se refiere a datos almacenados por el destinatario 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 abusivo. Además, existe un motivo de denegación que sólo es aplicable a la orden europea de entrega y es que, solicitándose datos de transacciones y de contenido, la infracción penal no sea de las que permiten la entrega de este tipo de datos.

Ver Texto

- (36) Debido al mayor grado de injerencia en los derechos de las personas afectadas.

Ver Texto

- (37) Cfr. el Considerando 52.

Ver Texto

- (38) Cfr. el Considerando 53 y la explicación de los arts. 15 y 16 de la Exposición de Motivos.

Ver Texto



(39) 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*).

[Ver Texto](#)

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

[Ver Texto](#)

(41) Con evidente error, el propio art. 5.7 incluye en su parte final los datos relativos al acceso, junto a los datos de transacciones o de contenido solicitados.

[Ver Texto](#)

(42) *Clarifying Lawful Overseas Use of Data*, de 23 de marzo de 2018 (Ley de aclaración del uso legítimo de los datos en el extranjero).

[Ver Texto](#)

(43) 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.

[Ver Texto](#)