III

2021 N.º 135

cuadernos de política criminal

segunda época

Dykinson, S.L.

III

2021 N.º 135

cuadernos de política criminal

segunda época

Edita

Dykinson, S.L.

AVISO IMPORTANTE A NUESTROS SUSCRIPTORES

Si desea suscribirse a **Cuadernos de Política Criminal**, llame por teléfono o envíe un e-mail a info@dykinson.com, indicando la forma de pago y el número o números a los que quiere suscribirse, e inmediatamente recibirá su pedido.

CPC se adhiere a las Core Practices del Committee on Publication Ethics (COPE) disponibles en: *https://publicationethics.org/core-practices*; y especialmente a los *Principios de Buenas Prácticas y Transparencia en las Publicaciones Académicas* desarrollados por el Committee on Publication Ethics (COPE), Open Access Scholarly Publishers Association (OASPA), Directory of Open Access Journals (DOAJ) y World Association of Medical Editors (WAME) disponibles en: *https://publicationethics.org/ resources/guidelines-new/principles-transparency-and-best-practice-scholarly-publishing*

La Revista no se responsabiliza de las opiniones contenidas en los artículos

Edita: Dykinson, S.L.
C/ Meléndez Valdés, 61 — 28015 Madrid
Tels. 91 544 28 46 / 91 544 28 69
Fax 91 544 60 40
info@dykinson.com / www.dykinson.com

Imprime: Safekat, S. L.
Laguna del Marquesado, 32 - 28021 Madrid
www.safekat.com

ISSN: 0210-4059
Depósito Legal: M. 7533-1977

CONTENIDO

SECCIÓN BIBLIOGRÁFICA

SECCION DERECHO COMPARADO Y DERECHO INTERNACIONAL PENAL

LAS ÓRDENES EUROPEAS DE ENTREGA Y CONSERVACIÓN: LA FUTURA OBTENCIÓN TRANSNACIONAL DE LA PRUEBA ELECTRÓNICA EN LOS PROCESOS PENALES EN LA UNIÓN EUROPEA

The european production and preservation orders: the future cross-border access to electronic evidence in criminal proceedings in the European Union

ÁNGEL TINOCO PASTRANA*

Fecha de recepción: 26/10/2021
Fecha de aprobación: 28/11//2021

RESUMEN: En este artículo se estudia la propuesta de la Unión Europea para la creación de un nuevo instrumento para la obtención transna-

* Profesor Titular de Derecho Procesal, Universidad de Sevilla. ORCID ID: https://orcid.org/0000-0002-6622-9030. El presente trabajo se enmarca dentro del Proyecto de Investigación "La evolución del espacio judicial europeo en materia civil y penal: su influencia en el proceso español", Proyecto I+D, PGC2018-094209-B-I00, Ministerio de Educación, Agencia Estatal de Investigación. Esta investigación fue iniciada en una estancia realizada en el *European University Institute* (Florencia) en 2018, financiada por el VI Plan Propio de Investigación de la Universidad de Sevilla.

cional de la prueba electrónica en materia penal. Con ello, se pretenden afrontar los actuales y relevantes retos en materia de lucha contra la ciberdelincuencia y el terrorismo internacional, instaurándose un nuevo modelo de cooperación directa con los proveedores de servicios de telecomunicaciones en el Espacio Europeo de Libertad, Seguridad y Justicia. Las nuevas órdenes europeas de entrega y conservación de pruebas electrónicas, introducen una nueva concepción o reinterpretación del principio de reconocimiento mutuo, que requiere un alto nivel de confianza mutua. Para ello es prioritario el respeto del principio de proporcionalidad y que se creen las necesarias salvaguardias para la protección de los derechos fundamentales y garantías procesales.

PALABRAS CLAVE: prueba transnacional electrónica, orden europea de entrega, orden europea de conservación, ciberdelincuencia, proveedores de servicios, principio de reconocimiento mutuo, derechos fundamentales

ABSTRACT*: *This paper studies the proposal of the European Union for the creation of a new instrument for cross-border access to electronic evidence in criminal matters. With this, it is intended to face the current and relevant challenges in the fight against cybercrime and international terrorism, establishing a new model of direct cooperation with telecommunications service providers in the European Area of Freedom, Security and Justice. The new European Orders for the production and preservation of electronic evidence introduce a new conception or reinterpretation of the principle of mutual recognition, which requires a high level of mutual trust. For this, respect for the principle of proportionality is a priority and that the necessary safeguards are created for the protection of fundamental rights and procedural guarantees.

KEYWORDS: electronic transnational evidence, European Production Order, European Preservation Order, cybercrime, service providers, principle of mutual recognition, fundamental rights.

I. CONSIDERACIONES PRELIMINARES

La creación de un instrumento para la obtención transnacional de la prueba electrónica en la Unión Europea (UE), constituye una cuestión

apremiante y prioritaria en el Espacio de Libertad, Seguridad y Justicia (ELSJ). En la actualidad existe un marco normativo insuficiente y fragmentario en la materia, para dar respuesta a las necesidades existentes en la lucha contra las distintas formas de delincuencia transnacional, sobre todo contra las formas más graves de ciberdelincuencia y el terrorismo. Y ello a pesar de la relativamente reciente Orden Europea de Investigación (OEI), que permite la práctica de diligencias de investigación tecnológica, ya que se cuestiona si este instrumento es suficiente para satisfacer las necesidades actuales. La propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las Órdenes Europeas de Entrega y de Conservación de pruebas electrónicas a efectos de enjuiciamiento penal, tiene como objetivo solventar esta situación, constituyendo un nuevo instrumento de cooperación judicial que coexistiría tanto con la OEI como con la asistencia judicial, si bien las futuras órdenes presentan notables diferencias tanto en su concepción como en su funcionamiento e incardinación en el ELSJ, respecto a los clásicos instrumentos de reconocimiento mutuo.

En abril de 2018, la Comisión Europea presentó dos propuestas legislativas para mejorar la obtención transnacional de la prueba electrónica en los procesos penales en la UE. Se trata de la propuesta de Reglamento sobre las Órdenes Europeas de Entrega y de Conservación y de la propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales[1]. Éstas constituyen el paquete sobre pruebas electrónicas presentado por la Comisión con el objetivo de que las autoridades policiales y judiciales puedan obtener las pruebas electrónicas con mayor agilidad y rapidez, siendo formuladas tras la petición que se le efectuó al respecto en las conclusiones del Consejo de la Unión Europea de 20 de noviembre de 2017[2], para que efectuara una propuesta legislativa en la materia a principios de 2018.

---

[1] Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las Órdenes Europeas de Entrega y Conservación de pruebas electrónicas a efectos de enjuiciamiento criminal, COM (2018) 225 final, 17 de abril de 2018, 2018/0108 (COD) y Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, COM (2018), 226 final, 17 de abril de 2018, 2018/0107 (COD).

[2] Respecto a las conclusiones de dicho Consejo de la Unión Europea (doc. nº 14435/17), véase: *https://www.consilium.europa.eu/media/31666/st14435en17.pdf* (fecha de consulta: 3 de diciembre de 2021).

La Comisión Europea cuando hizo pública las propuestas, destacó la creciente importancia de las pruebas electrónicas para los procesos penales, que actualmente las solicitudes transfronterizas para obtenerlas predominan en las investigaciones y, que no puede permitirse que los delincuentes y terroristas exploten las tecnologías modernas de comunicación para ocultar sus actividades y eludir la acción de la justicia. También observó que las autoridades continúan trabajando con métodos complicados y, que si bien son necesarias la cooperación judicial y asistencia mutua, en la actualidad el proceso es demasiado lento y complejo, mientras que los delincuentes recurren a tecnologías de vanguardia, debiéndose dotar a las autoridades de métodos del s. XXI, dado que aproximadamente dos tercios de las pruebas electrónicas están localizadas en otro Estado (tanto dentro como fuera de la UE), lo cual obstaculiza tanto la investigación como el enjuiciamiento[3], surgiendo por tanto numerosos retos para la jurisdicción de cada Estado, dado que Internet carece de fronteras.

El Consejo de la Unión Europea adoptó su posición respecto a la propuesta de Reglamento de la Comisión, en el Consejo de Justicia y Asuntos de Interior de 7 de diciembre de 2018, la cual constituye la orientación del Consejo de la Unión Europea sobre la propuesta de Reglamento y, la base para entablar las negociaciones con el Parlamento. Posteriormente la orientación general fue complementada con los respectivos anexos añadidos por el Consejo de la Unión Europea Justicia y Asuntos de Interior de 6 de junio de 2019[4]. Ésta constituye fundamentalmente la versión de la propuesta de Reglamento que vamos a utilizar para estudiar en el presente trabajo la Orden Europea de Entrega (OEE) y la Orden Europea de Conservación (OEC), si bien haremos las oportunas referencias tanto a la propuesta de la Comisión Europea como a la postura adoptada en los actuales trabajos parlamentarios.

En cuanto a la propuesta de Directiva de la Comisión para la designación de los representantes legales, instrumento fundamental para la aplicación de la OEE y de la OEC, el Consejo de la Unión Europea aprobó su posición en el Consejo de Justicia y Asuntos de Interior de 8 de marzo de 2019, la cual constituye igualmente la orientación general del Consejo para entablar las negociaciones con el Parlamento Europeo[5]. Del mismo

[3] Así se refleja en comunicado de prensa de la Comisión Europea de 17/04/2018: *https://ec.europa.eu/commission/presscorner/detail/es/IP_18_3343* (fecha de consulta: 3 de diciembre de 2021).

[4] Véanse, Consejo de la Unión Europea, nº documento 15292/18, de 12/12/2018 y Consejo de la Unión Europea, nº documento 10206/19, de 11/06/2019.

[5] Consejo de la Unión Europea, nº documento 6946/19, de 28/02/2018.

modo, esta versión de la propuesta de Directiva será la que fundamentalmente seguiremos en el presente estudio.

En el Parlamento Europeo, tanto la propuesta de Reglamento como de Directiva de la Comisión Europea, se han asignado a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (Comisión LIBE), que aprobó los respectivos informes sobre dichas propuestas el 7 de diciembre de 2020[6]. En la posición final del informe de la Comisión LIBE sobre la propuesta de Reglamento de la Comisión Europea, se incorporan numerosas enmiendas[7]. Respecto a la propuesta de Directiva de la Comisión Europea, quizá lo más significativo de la posición de la Comisión LIBE, consiste en que se rechaza la propuesta de la Comisión Europea, pidiéndose que la retire, integrando su contenido en el Reglamento, lo cual lo fundamenta en que plantea problemas jurídicos, conforme a lo establecido en los artículos 53 y 62 del Tratado de Funcionamiento de la Unión Europea (TFUE). De este modo, sólo los Estados que participen en el Reglamento estarían obligados al nombramiento de los representantes legales[8].

La regulación de la OEE y OEC por un Reglamento, pone de manifiesto que la UE no está dispuesta en el ámbito del ELSJ, a que la efectividad de los instrumentos pudiera verse obstaculizada por la extemporánea o falta de transposición de los Estados, riesgos que existen con la Directiva[9], como sucedió, por ejemplo, con la Directiva 2014/41/UE, reguladora de la Orden Europea de Investigación, además de fortalecerse la seguridad jurídica

[6] Ponente Birgit Sippel, Proyectos de Informes y enmiendas, LIBE/9/00283 y LIBE/9/00281. Véase *https://emeeting.europarl.europa.eu/emeeting/committee/es/agenda/202012/LIBE?meeting=LIBE-2020-1207_1&session=12-07-09-00* (fecha de consulta: 3 de diciembre de 2021).

[7] Informe (A9-0256/2020), confirmado por el Pleno el 16/12/2020. Se acordó, entre otras cuestiones: la notificación obligatoria al Estado de ejecución; modificar las categorías de datos; introducir motivos para el no reconocimiento o no ejecución; reforzar los recursos efectivos; extender el plazo para casos de emergencia a dieciséis horas y proporcionar un sistema de intercambio común de la UE para la transmisión de los datos solicitados. Véase: *https://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders* (fecha de consulta: 3 de diciembre de 2021).

[8] Informe (A9-0257/2020), confirmado por el Pleno el 16/12/2020. Véase: *https://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-jd-cross-border-access-to-e-evidence-appointment-of-legal-representatives* (fecha de consulta: 3 de diciembre de 2021).

[9] Un ejemplo reciente es la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), de 25 de febrero de 2021, por la que se condena a España por la falta de transposición de la Directiva (UE) 2016/680, de protección de datos en los procesos penales, finalmente transpuesta, por la Ley Orgánica 7/2021, de 26 de mayo.

evitándose interpretaciones divergentes por los Estados[10]. Ello nos muestra la orientación que la UE está siguiendo en el ámbito del ELSJ, como se refleja en otros instrumentos recientes como la creación de la Fiscalía Europea a través del Reglamento (UE) 2017/1939 o en el Reglamento (UE) 2018/1805, sobre el reconocimiento mutuo de resoluciones de embargo y decomiso. Sin embargo, respecto a la designación de los representantes legales de los proveedores de servicios, fundamentales para el funcionamiento de la OEE y la OEC, la Comisión y el Consejo han optado por una Directiva con un plazo de dieciocho meses de transposición[11], lo cual podría constituir un obstáculo para la efectividad de dichas órdenes. Por ello valoramos positivamente la postura de la Comisión LIBE, que integra el contenido de la Directiva en el Reglamento.

Entre las prioridades legislativas comunes delimitadas en la Declaración Conjunta de las tres instituciones de la UE para 2021, se incorporan expresamente tanto la creación de la OEE y OEC como el nombramiento de los representantes legales para la obtención de pruebas electrónicas[12]. Ello refleja la relevancia y actualidad de la materia[13],

---

[10] Fuentes Soriano, O. (2020). "Capítulo 2. Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas", en O. Fuentes Soriano (Dir.), Era digital, sociedad y Derecho, Tirant lo blanch, Valencia, págs. 288-289. El Reglamento supera los niveles conseguidos con la clásica vía de la cooperación judicial, teniendo la ventaja de afrontar las dificultades de establecer una cooperación fiable entre las autoridades y los proveedores de servicios. Además, Rogalski, M. (2020). "The European Commission´s e-Evidence Proposal. Critical Remarks and Proposal for Changes". European Journal of Crime, Criminal Law and Criminal Justice, nº vol. 28, nº 4, págs. 333-336, resalta beneficios como la uniformidad en la materia, dado el delicado balance entre la eficiencia en las investigaciones, la certeza legal para las compañías tecnológicas y la protección de los derechos.

[11] Según el art. 7.1 de la Orientación General del Consejo sobre la Propuesta de Directiva de la Comisión (en adelante, PDOGC). Este plazo ha sido ampliado respecto al establecido en el art. 7.1 de la Propuesta de Directiva de la Comisión (en adelante, PDC), donde el plazo de transposición se fijaba en seis meses.

[12] Véase, *https://oeil.secure.europarl.europa.eu/oeil/popups/thematicnote.do?id=2066000&l=en* (fecha de consulta: 3 de diciembre de 2021), referencias de procedimiento legislativo 2018/0108 (COD) y 2018/0107 (COD), respectivamente, propuestas que se encuentran a la espera de la posición del Parlamento en primera lectura.

[13] Jour-Schöroder, A. (2020). "Guest Editorial". EUCRIM, nº 3, pág. 157. Disponible en: *https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf#page=3* (fecha de consulta: 3 de diciembre de 2021), la Comisión Europea continuará negociando las propuestas de pruebas electrónicas para concluir el procedimiento legislativo a la mayor brevedad, lo cual permitiría, la reanudación de las negociaciones con EE.UU. en la materia. La Comisión pretende además potenciar el diálogo con los expertos sobre el desarrollo de las futuras políticas en materia probatoria, como el *Criminal Policy Group*.

a pesar de haberse observado cierta ralentización de los trabajos en el Parlamento[14], como consecuencia, entre otros factores, de su renovación en 2019 e incluso por la incidencia de la pandemia.

Como principales innovaciones que suponen la OEE y la OEC, se pueden destacar la gran simplificación del procedimiento respecto a los actuales instrumentos y mecanismos. La OEE y la OEC, permiten que la autoridad del Estado de emisión, ordene directamente a un proveedor de servicios que los ofrezca en la UE, a que entregue o conserve las pruebas electrónicas, con independencia de dónde se ubiquen los datos, no pudiendo suponer el Reglamento, la modificación de la obligación de respetar los principios y derechos fundamentales contenidos en el art. 6 del Tratado de la Unión Europea (TUE), incluyendo el derecho de defensa[15]. En la OEE se reducen notoriamente los plazos para la entrega de la prueba electrónica, en diez días con carácter general y seis horas para los casos urgentes, desde la recepción del certificado[16], lo cual supone un importante avance respecto a los ciento veinte días que supone la OEI y los diez meses en el ámbito de la asistencia judicial[17], constituyendo un indudable acierto la posibilidad de conservarlos a través de la OEC. No obstante, se podrá continuar emitiendo la OEI para la obtención de pruebas electrónicas, aunque entren dentro del ámbito de aplicación del Reglamento e incluso los cauces de asistencia mutua existentes[18].

---

[14] No estamos ante instrumentos que previsiblemente vayan a estar en funcionamiento a corto plazo; tras la entrada en vigor del Reglamento, su plazo de aplicación se establece en seis meses en el art. 22 de la Propuesta de Reglamento de la Comisión (en adelante, PRC), veinticuatro meses en el art. 22 de la Orientación general del Consejo sobre la Propuesta de Reglamento (en adelante, PROGC) y dieciocho meses en el art. 22 de la posición adoptada por la Comisión LIBE sobre la Propuesta de Reglamento (en adelante, PRLIBE).

[15] Véase art. 1 PRC y PROGC. En el art. 1 PRLIBE entre otras innovaciones, se incluye la referencia a los derechos fundamentales y principios consagrados en la Carta de Derechos Fundamentales de la Unión Europea (CDFUE). Como destaca González Granda, P. (2021). "Capítulo 35. Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal: próximo avance en materia de prueba penal transfronteriza", en V. Moreno Catena y M. I. Romero Pradas (Dirs.), Nuevos postulados de la Cooperación Judicial en la Unión Europea, Libro homenaje a la Profª. Mª Isabel González Cano, Tirant lo blanch, Valencia, págs. 1096-1099, constituye una preocupación reiterada en el texto de la propuesta (PRC) la protección de los derechos fundamentales, efectuándose referencia expresa a los derechos contenidos en los arts. 47 y 48 CDFUE y al problema de que en terceros Estados no exista un similar nivel de protección de estos Derechos que en la UE.

[16] Art. 9.1 y .2 PROGC. En los arts. 8 bis.3 y 9.2 ter PRLIBE, se amplía el último plazo a dieciséis horas.

[17] Véase entre otros, el *Factsheet e-evidence*: *https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345* (fecha de consulta: 3 de diciembre de 2021).

[18] *Cfr.* art. 23 PRC, PROGC y PRLIBE.

Existen importantes diferencias entre la OEE y OEC respecto a los actuales instrumentos de reconocimiento mutuo, dado que sus certificados se notificarán directamente al proveedor de servicios del Estado de ejecución (art. 7.1 PROGC y PRC) y, por tanto, no a una autoridad del mismo[19], lo cual podría conllevar una importante evolución en materia de confianza mutua en el ELSJ. Tampoco existe, por ejemplo, referencia alguna a la clásica lista de treinta y dos delitos en los que no se efectuará el control de la doble tipificación, existente en los actuales instrumentos de reconocimiento mutuo. Desde esta perspectiva observamos que la OEE y la OEC no constituirían como tales instrumentos de reconocimiento mutuo *stricto sensu*, si bien estaríamos ante instrumentos de cooperación judicial en materia penal que requieren un "alto nivel de confianza mutua entre los Estados miembros" (Considerando nº 11 Exposición de Motivos PROGC y PRC). Podrían conceptuarse como un nuevo tipo de instrumento de cooperación judicial o como un nuevo subtipo o categoría de instrumento de reconocimiento mutuo. Pero ello sólo sería extrapolable respecto a la PRC y la PROGC, dado que en la PRLIBE y únicamente respecto a la OEE, se reproduce la exclusión del control de la doble tipificación de la misma forma que en los clásicos instrumentos de reconocimiento mutuo (art. 10 bis.2, b), versión donde las órdenes se transmitirán simultáneamente tanto al proveedor de servicios como la autoridad de ejecución (arts. 7.1, 8 bis.1 y 9.1 bis PRLIBE).

Tras estas consideraciones sobre la propuesta de la OEE y OEC y las posturas adoptadas al respecto en seno de las instituciones de la UE, va-

[19] Ello, está siendo muy controvertido en diversos foros, lo cual, en gran medida, ha tenido como consecuencia la diversa postura adoptada por la Comisión LIBE. Stefan, M. y González Fuster, G. (2018). "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 Papers in Liberty and Security in Europe, nº 07, November (updated in May 2019), págs. 30-32. Disponible en: *https://www.ceps.eu/ceps-publications/cross-border-access-electronic-data-through-judicial-cooperation-criminal-matters/* (fecha de consulta: 3 de diciembre de 2021). En la evaluación de impacto se califica a las órdenes como "una nueva dimensión del reconocimiento mutuo". La Comisión argumenta que las órdenes introducen un "nuevo modelo" de directa "público-privada" cooperación en materia penal, que se basa en el principio de reconocimiento mutuo. Cuestionan que la ejecución de las órdenes por una empresa privada, se pueda calificar como auténtica "cooperación judicial" o como "forma de reconocimiento mutuo". Por ello está siendo controvertida la base jurídica elegida por la Comisión, el art. 82.1 TFUE. En el mismo sentido, entre otros, Robinson, G. (2018). "The European Comission´s e-Evidence Proposal". European data protection Law Review, vol. 4, nº 3, pág. 352. Igualmente considera que existe un gran obstáculo en la base jurídica de la propuesta, siendo este nuevo instrumento fácilmente impugnable ante el TJUE.

mos a contextualizar este instrumento en el marco de otras actuaciones e iniciativas que se están desarrollando en la UE.

II. CONTEXTO DE LA PROPUESTA Y ACTUACIONES COMPLEMENTARIAS

En la UE existen otras actuaciones estrechamente relacionadas con la prueba electrónica. En el Consejo de la Unión Europea de 8 de marzo de 2019, antes referido, también se debatió sobre otras medidas relevantes para completar la normativa sobre pruebas electrónicas, en concreto, para asegurar el rápido y eficaz acceso a las pruebas que se almacenen fuera de la UE. Dichas medidas, consisten en los mandatos para negociar el Segundo Protocolo adicional al Convenio de Budapest y un Acuerdo entre la UE y los Estados Unidos (EE.UU.)[20].

Ya se abordó previamente esta cuestión en el Consejo de la Unión Europea de 4 y 5 de junio de 2018, donde se acordó continuar con los contactos y negociaciones con EE.UU. y que se presentara de forma urgente un mandato de negociación con EE.UU., dada la reciente promulgación de la *US Cloud Act* "Ley de clarificación del uso legítimo de los datos fuera de los Estados Unidos" (23 de marzo de 2018), norma prácticamente coetánea a la entrada en vigor del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), con el que puede presentar conflictos. Los mandatos de negociación referidos se otorgaron de forma efectiva a la Comisión Europea en el Consejo de la Unión Europea de 6 de ju-

[20] Fuentes Soriano, O. (2020). *Op. cit.*, pág. 295. Actualmente la cooperación entre las autoridades de los Estados de la UE y los proveedores instalados en EE.UU., que colaboran de forma voluntaria, se centra en los "datos sin contenido", lo cual genera inseguridad jurídica y repercute en las garantías procesales. En este sentido Bueno de Mata, F. (2021). "Capítulo 1. Análisis de las medidas de cooperación judicial internacional para la obtención transfronteriza de pruebas en materia de cibercrimen", en L. Fontestad Portalés (Dir.), La transformación digital de la cooperación jurídica penal internacional, Thomson Reuters Aranzadi, Cizur Menor, pág. 42, considera que el Acuerdo con EE.UU. constituiría un "hito histórico". El Acuerdo con EE.UU. permitiría instaurar una auténtica "cooperación procesal mundial" en el ámbito del ciberespacio y la creación de "Códigos Modelo" (pág. 46). También, Gómez Amigo, L. (2019). "Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima". Revista Española de Derecho Europeo, nº 71, págs. 51-53. Disponible en: *http://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/view/47/69* (fecha de consulta: 3 de diciembre de 2021), que destaca que uno de los objetivos del Acuerdo entre la UE y EE.UU., consiste en evitar obligaciones contradictorias entre ellos, Acuerdo que sería posible al amparo de la *US Cloud Act*.

nio de 2019[21], en los cuales se incorporan relevantes garantías respecto a los derechos fundamentales, la privacidad y los derechos procesales. En el mandato para negociar el acuerdo con EE.UU. se consideran especialmente los conflictos legales y las reglas comunes para la transferencia directa y recíproca de la prueba, el cual se suma al mandato para participar en las negociaciones con el Consejo de Europa en relación a un segundo Protocolo Adicional al Convenio de Budapest sobre la Ciberdelincuencia, recientemente aprobado por el Comité de Estados Parte[22]. La ciberdelincuencia y el terrorismo, entre otras formas de delincuencia transnacional, constituyen fenómenos globales, dimensión que también adquiere el acceso a la prueba electrónica, siendo fundamental la colaboración con terceros Estados a través de la vía convencional, sobre todo con EE.UU.[23], donde transitan y/o se almacenan gran parte de los datos electrónicos[24].

En el ELSJ el acceso a los datos electrónicos ha adquirido un protagonismo esencial, respecto a los que versan estos nuevos instrumentos, con el objetivo fundamental de preservar la seguridad. Dentro del trinomio "libertad, seguridad y justicia", la seguridad posee una posición prevalente en la UE. Se ha observado que en el ELSJ existe una necesidad urgente de reconciliar la seguridad con las nociones de libertad y justicia, para evitar que sus compromisos se deterioren y acaben bajo un formalismo vacío, pudiéndose conseguir una noción integrada de la justicia aplicando la proporcionalidad para fomentar la equidad de todo el sistema[25]. Si bien

---

[21] Sobre dichos Consejos de la UE: *https://www.consilium.europa.eu/es/meetings/jha/2019/03/07-08/; https://www.consilium.europa.eu/es/meetings/jha/2018/06/04-05/; https://www.consilium.europa.eu/es/meetings/jha/2019/06/06-07/* (fecha de consulta: 3 de diciembre de 2021).

[22] Fue aprobado el 28/05/2021, véase: *https://rm.coe.int/0900001680a2aa1c* (fecha de consulta: 3 de diciembre de 2021).

[23] Jimeno Bulnes, M. (2019). "Capítulo XXXV. La prueba transfronteriza y su incorporación al proceso penal español", en M. I. González Cano (Dir.), Orden Europea de investigación y prueba transfronteriza en la Unión Europea, Tirant lo blanch, Valencia, págs. 719, 759-761. Una de las "pistas fundamentales" sobre la propuesta normativa de las órdenes europeas sobre pruebas electrónicas, es la referencia que se efectúa en la Exposición de Motivos a EE.UU., que es quien recibe "el mayor número de solicitudes de la UE", siendo el "leit-motiv" de la propuesta. Esta nueva regulación no sustituye a la OEI, aunque ésta según determinadas asociaciones de protección de los derechos humanos, sería suficiente para conseguir los mismos fines que las nuevas órdenes.

[24] Véase sobre los referidos mandatos de negociación y el contexto expuesto: *https://ec.europa.eu/commission/presscorner/detail/es/IP_19_2891* (fecha de consulta: 3 de diciembre de 2021).

[25] *Vid*. Herlin-Karnel, E. (2017). "The domination of security and the promise of justice: on justification and proportionality in Europe´s ´Area of Freedom, Security and Justice´". Transnational Legal Theory, vol. 8, nº 79, págs. 83 y 87-90. Disponible en:

se considera apremiante la creación de instrumentos para la obtención transnacional de la prueba electrónica, es necesario que la justicia y la libertad se pongan en valor en el ELSJ, para lo cual el principio de proporcionalidad constituiría un elemento fundamental.

La relevancia de la seguridad se refleja en que se puede afirmar respecto al paquete sobre pruebas electrónicas, que la lucha contra el terrorismo constituye la cuestión fundamental que lo impulsó, como se refleja en el desarrollo cronológico de las distintas actuaciones. El germen de la propuesta de la Comisión, lo encontramos en la "Declaración conjunta de los Ministros de Justicia y Asuntos de Interior de la UE y los representantes de las instituciones de la UE", de 24 marzo de 2016, dos días después de los atentados terroristas de Bruselas, donde entre otras medidas, se considera prioritario fomentar la obtención rápida y eficaz de pruebas digitales[26]. A continuación el 9 de junio de 2016, el Consejo de la Unión Europea, adoptó las "Conclusiones sobre la mejora de la justicia penal en el ciberespacio" y las "Conclusiones sobre la Red judicial europea de delincuencia informática", donde expresamente se resaltó el aumento de la relevancia de las pruebas electrónicas en los procesos penales sobre todo en materia de terrorismo, la necesidad de racionalizar los procedimientos de asistencia judicial y el reconocimiento mutuo y, la mejora de la cooperación con los proveedores de servicios[27]. Pero fue en el Consejo Europeo de 22 y 23 de junio de 2017 cuando se concluye que el acceso transfronterizo a las pruebas electrónicas es primordial para la lucha contra la delincuencia grave y el terrorismo[28], tras el cual en el Consejo de 20 de noviembre se pidió a la Comisión que efectuara una propuesta legislativa a principios de 2018, como hemos visto[29].

Como otras actuaciones relacionadas que se están llevando a cabo actualmente y, que además forman parte de la respuesta de la UE a la amenaza terrorista[30], destacamos la reciente adopción del Reglamento

https://www.tandfonline.com/doi/pdf/10.1080/20414005.2017.1316637?needAccess=true (fecha de consulta: 3 de diciembre de 2021).

[26] *Cfr*: *https://www.consilium.europa.eu/es/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/* (fecha de consulta: 3 de diciembre de 2021).

[27] Véase: *https://www.consilium.europa.eu/es/press/press-releases/2016/06/09/criminal-activities-cyberspace/* (fecha de consulta: 3 de diciembre de 2021).

[28] Sobre las conclusiones: *https://www.consilium.europa.eu/media/23969/22-23-euco-final-conclusions-es.pdf* (fecha de consulta: 3 de diciembre de 2021).

[29] Respecto al íter y antecedentes relacionados, véase además: https://www.consilium.europa.eu/es/policies/e-evidence/ (fecha de consulta: 3 de diciembre de 2021).

[30] Sobre estas medidas, donde entre otras, se encuentra la digitalización de la cooperación judicial: *https://www.consilium.europa.eu/es/policies/fight-against-terrorism/* (fecha de consulta: 3 de diciembre de 2021).

(UE) 2021/784 del Parlamento Europeo y del Consejo de 29 de abril, para la lucha contra la difusión de contenidos terroristas en línea, aplicable a partir del 7 de junio de 2022. Este Reglamento faculta a las autoridades competentes de los Estados miembros para que emitan órdenes de retirada o de bloquear contenidos terroristas en el reducido plazo de una hora, dirigidas a los proveedores de servicios que los ofrezcan en la UE. Vemos como tanto los datos electrónicos como los proveedores de servicios ostentan una posición fundamental en dicho Reglamento, constituyendo piezas clave, del mismo modo que en la propuesta sobre la OEE y la OEC, la cual está contemplada expresamente, entre otras actuaciones, en la nueva "Estrategia de ciberseguridad de la UE para la década digital", presentada en diciembre de 2020, respecto a la cual el Consejo de la Unión Europea adoptó sus conclusiones en marzo de 2021, al igual que en la "Estrategia Europea para hacer frente a la delincuencia organizada", presentada por la Comisión Europea el 14 de abril de 2021[31].

Hemos contextualizado la génesis y evolución de la propuesta sobre la obtención transnacional de la prueba electrónica en materia penal, del mismo modo que hemos resaltado determinadas características fundamentales. A continuación, vamos a estudiar la OEE, la OEC y la designación de los representantes legales de las empresas proveedoras de servicios.

III. LA ORDEN EUROPEA DE ENTREGA

1. Concepto

La OEE constituye un instrumento por el que la autoridad emisora de un Estado miembro, obliga de forma vinculante[32] a un provee-

[31] Respecto a dicha Estrategia, *https://ec.europa.eu/commission/presscorner/detail/es/IP_21_1662*; en relación a la Estrategia formulada por la Comisión y el Alto Representante para Asuntos Exteriores: *https://www.consilium.europa.eu/es/policies/cybersecurity/* y las referidas las conclusiones del Consejo: *https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf* (fecha de consulta: 3 de diciembre de 2021). Otras iniciativas legislativas estrechamente relacionadas con esta materia, son las recientes Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial de 21/04/2021 y, la Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a un mercado único de servicios digitales de 15/12/2020. También tenemos que referir el marco creado por el reciente Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021, por el que se establece el Programa Europa Digital (2021-2027), dada su relación con las referidas iniciativas.

[32] Gialuz, M. y Della Torre, J. (2018). "Lotta alla criminalità nel cyberspazio: La Commissione presenta due proposte per facilitare la circulazione delle prove elettroniche nei processi penali". Diritto penale contemporaneo, nº 5, pág. 281. Disponible en:

dor[33] que preste servicios de comunicaciones electrónicas, servicios de asignación de nombres de dominio de internet y de direcciones IP y otros servicios de la sociedad de la información en la UE[34], que esté establecido o representado en el territorio de otro Estado miembro[35], a que entregue pruebas electrónicas (art. 2.1), 3) PROGC)[36]. Éstas consisten en pruebas

https://archiviodpc.dirittopenaleuomo.org/upload/9339-gialuzdellatorre2018a.pdf (fecha de consulta: 3 de diciembre de 2021). Las autoridades nacionales han comenzado a contactar de forma directa con los proveedores de servicios, tanto en la UE como en terceros Estados, sin intervención de la autoridad del Estado de ejecución, instaurándose una vía de transmisión voluntaria de la prueba electrónica. También, Robinson, G. (2018). *Op. cit*., págs. 347-348. La cooperación entre las autoridades y las empresas privadas, puede plantear problemas procesales y en la protección de datos, conllevando la extensión extraterritorial de las facultades de investigación nacionales a través de actores privados. Tosza, S. (2020). "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order". New Journal of European Criminal Law, vol. 11, nº 2, págs. 168-170. Disponible en: *https://journals.sagepub.com/doi/full/10.1177/2032284420919802* (fecha de consulta: 3 de diciembre de 2021). El enfoque territorial de la jurisdicción fundamentado en la ubicación de los datos, está desactualizado, dado el incremento del uso de la "nube" y su facilidad de transmisión. Las autoridades dependen enormemente de la cooperación de los proveedores. Ello se suma a la volatilidad de los datos y las insuficiencias de la OEI con extensos plazos, lo cual justifica la propuesta de Reglamento, donde se abandona el principio de territorialidad.

[33] En el art. 2.1 PRLIBE, se innovan las definiciones, estableciéndose que se trata de una decisión "emitida o validada por una autoridad judicial" del "Estado emisor", que el proveedor debe estar en otro Estado miembro, "Estado de ejecución", asimilándose a las instituciones habituales en los instrumentos reconocimiento mutuo.

[34] Se exceptúan expresamente los servicios financieros referidos en el art. 2.2, b) de la Directiva 2006/123/CE (art. 2.3) PROGC). Las definiciones están en consonancia con las establecidas en el acervo normativo de la UE en materia de datos, lo cual contribuye a la coherencia del sistema. El concepto de "servicios de comunicaciones electrónicas" se determina según el art. 2.4 de la Directiva (UE) 2018/1972 y, los "otros servicios de la sociedad de la información", son los establecidos en el art. 1,1 b) de la Directiva (UE) 2015/1535.

[35] El concepto de "ofrecer servicios en la Unión" se determina por la posibilidad de utilizar los servicios en los Estados miembros y la vinculación con los mismos (art. 2.4) PROGC) y el de "establecimiento o estar establecido", conlleva el ejercicio de la actividad indefinidamente a través de una infraestructura estable (art. 2.5 PROGC). Véanse, además, sobre estos conceptos, Geraci, R. M. (2019). "La circulazione transfrontaliera delle prove digitali in UE: La proposta di Regolamento e-evidence". Cassazione penale, vol. 59, nº 3, pág. 1134 y Tosza, S. (2020). *Op. cit*., págs. 172-173, que cuestiona que la mera accesibilidad del servicio en la UE constituya un criterio suficiente, al conllevar que todos los proveedores del mundo entrarían dentro del ámbito de aplicación.

[36] Ello se ordenará con independencia de donde se ubiquen los datos (art. 1.1 PROGC). Fuentes Soriano, O. (2020). *Op. cit*., pág. 297. La OEE sólo es aplicable respecto a proveedores que presten sus servicios en Estados diferentes al de emisión, no pudiéndose utilizar la OEE en entornos nacionales. Los servicios pueden prestarse o almacenarse desde cualquier lugar, la obtención de los datos con la OEE constituye un importante avance

almacenadas en formato electrónico por el proveedor de servicios o en su nombre[37], en el momento de la recepción del certificado de la OEE (EPOC)[38], consistentes en datos de abonados, de acceso, de transacciones y de contenido (art. 2.6 PROGC)[39]. Por tanto, se excluye la obtención de datos en tiempo real, es decir, no almacenados, por lo cual para la interceptación en el acto de las telecomunicaciones habría que emitir una

---

que inaugura un "nuevo escenario de actuación procesal" (págs. 292-293). Pero al reducirse la supervisión por las autoridades del Estado receptor a un control "meramente eventual", ello supondría la "privación" del reconocimiento mutuo (pág. 307). En este sentido, Geraci, R. M. (2019). *Op. cit.*, págs. 1349-1350, considera que podríamos estar ante una "peculiar modulación inédita", del principio de reconocimiento mutuo. La propuesta de Reglamento no armoniza ni aproxima las medidas de investigación nacionales, lo cual nos conduce a la eterna cuestión controvertida que existe en la cooperación judicial "post reconocimiento mutuo", que repercute en la efectiva confianza mutua (pág. 1360). También, entre otros, Daniele, M. (2019). "L´acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale". Revista Brasileira de Direito Processual Penal, vol. 5, nº 3, págs. 1282-1283. Disponible en: *http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/288/186* (fecha de consulta: 3 de diciembre de 2021). La cooperación directa con los proveedores, constituye un cambio en la filosofía de la cooperación, pudiéndose prever que ostente una importancia preeminente; Mitsilegas, V. (2018). "The privatisation of mutual trust in Europe´s área of criminal justice: The case of e-evidence". Maastricht Journal of European and Comparative Law, vol. 25, nº 3, pág. 264. Disponible en: *https://journals.sagepub.com/doi/pdf/10.1177/1023263X18792240* (fecha de consulta: 3 de diciembre de 2021). La cooperación directa entre las autoridades públicas y el sector privado, constituye un cambio paradigmático, que conduce a la privatización de la confianza mutua en Europa.

[37] Tosza, S. (2020). *Op. cit.*, págs. 171-173. Considera como una "técnica legislativa desafortunada", que la prueba electrónica se defina con el requisito de que esté disponible por el proveedor de servicios cuando se reciba la OEE, al tratarse en realidad de un aspecto del ámbito de aplicación del instrumento. La prueba electrónica tal y como está definida no constituye la única que existe, dado que versa sobre la recopilación de pruebas electrónicas en un determinado contexto y condiciones.

[38] En adelante, EPOC, según el acrónimo en inglés (art. 8.1 PROGC). Se diferencia entre la OEE como tal y su certificado o EPOC, siendo este último el que se transmite al destinatario para su ejecución.

[39] Las categorías de datos se definen en el art. 2.7) a 2.10) PROGC. En la PRLIBE (art. 2.6) a 10)) sin embargo, no se las trata como "pruebas electrónicas", sino como "información electrónica", se omite toda referencia a los datos de acceso y de transacciones, clasificándose los datos como "datos de abonados, de tráfico y de contenido", incorporándose los datos de acceso y transacciones como datos de tráfico. En esta versión, el momento que se considera respecto al almacenamiento de la información electrónica, es el de la emisión de la OEE, a diferencia de la PRC y PROGC. Observa Rogalski, M. (2020). *Op. cit.*, págs. 338-341, que las definiciones de "datos de acceso" y "datos de transacciones", efectuadas en la PRC, son imprecisas y presentan reiteraciones, proponiendo reformularlas, en aras de evitar interpretaciones ambiguas en la práctica.

OEI[40]. La OEE sólo podrá emitirse en el ámbito de los procesos penales[41], incluyéndose la ejecución de penas o medidas de seguridad privativas de libertad si no fueron dictadas en rebeldía cuando la persona condenada haya huido (la ejecución sólo se incorpora en el art. 3.2 PROGC). También podrá emitirse la OEE en procesos penales en los que una persona jurídica pueda ser responsable en el Estado emisor. Se excluyen expresamente los procesos que se inicien por la autoridad emisora para prestar asistencia mutua a otro Estado miembro o país tercero (art. 1 bis PROGC y PRLIBE).

El EPOC, incorporado como Anexo I en la PROGC, será cumplimentado por la autoridad competente para la emisión o validación de la OEE, la cual lo certificará y firmará (art. 8.1 PROGC). Inicialmente se prevé que el EPOC se transmita por cualquier medio seguro y fiable que permita constancia escrita y que determine su autenticidad o bien, la opción de la utilización de plataformas especializadas que pudieran crearse para ello (art. 8.2 PROGC). Pero en el PRLIBE (art. 8.2) se establece la obligatoriedad de utilizar el "Sistema europeo común de intercambio", que tendrá que crear la Comisión Europea para cuando entre en vigor el Reglamento (art. 7 bis PRLIBE), el cual estimamos que contribuirá muy favorablemente a la eficacia de este nuevo instrumento. Este Sistema no dependería de que los proveedores de servicios, Estados u organismos hubieran podido establecer una plataforma especializada o un canal, estando además previsto en el art. 7 bis.3 PRLIBE que, si dicha plataforma o canal hubiera sido creado, se tendrá que interconectar con el Sistema europeo común de intercambio[42]. El EPOC si fuera necesario, se tradu-

[40] Tosza, S. (2020). *Op. cit*., pág. 177, la OEI se fundamenta en la libre circulación de personas y la abolición de las fronteras, a diferencia de la OEE cuyo leitmotiv estriba en la inexistencia de fronteras en el ciberespacio, pudiendo ser necesaria una OEE respecto a un caso estrictamente interno, porque los datos que se requieren los posea un proveedor de servicios de otro Estado miembro.

[41] López Jiménez, R. (2019). "Nuevo marco transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas electrónicas". Revista General de Derecho Europeo, nº 49, págs. 325 y 327. Disponible en: *https://www--iustel--com.us.debiblio.com/v2/revistas/detalle_revista.asp?id_noticia=421898* (fecha de consulta: 3 de diciembre de 2021). La OEE no se puede emitir para la prevención de la delincuencia, sino dentro de un procedimiento penal y tampoco abarca procedimientos administrativos. Del mismo modo que en la OEI, la OEE no puede emitirse de forma prospectiva y responde al concepto de "orden" o "título ejecutivo europeo". Además, véanse Geraci, R. M. (2019). *Op. cit*., págs. 1344 y 1346 y Rogalski, M. (2020). *Op. cit*., pág. 337.

[42] La Comisión Europea presentó el 2/12/2020, la propuesta de Reglamento relativo a un sistema informatizado de comunicación en los procesos transfronterizos penales y civiles (sistema e-CODEX), por el que se modifica el Reglamento (UE) 2018/1726, adop-

cirá a una lengua oficial de la UE aceptada por el destinatario y si no hubiera concretado ninguna, a una lengua oficial del Estado miembro donde resida o esté establecido el representante legal (art. 8.5 PROGC). Cada Estado miembro deberá indicar si acepta para la ejecución, que se transmita el EPOC o la OEE en un idioma distinto a su lengua o lenguas oficiales, indicando cuál (art. 18 bis PROGC).

2. Autoridades competentes para la emisión

Cuando la OEE esté referida a datos de abonados y datos de acceso, podrá emitirse por un Juez, Tribunal, Juez de Instrucción o Fiscal[43], competentes en el asunto específico[44]. Estas mismas autoridades validarán la OEE cuando la emita cualquier otra autoridad competente según el Estado emisor, que en un asunto en concreto actúe como autoridad de investigación en procesos penales y pueda ordenar la obtención de pruebas conforme a su legislación nacional (art. 4.1 PROGC), lo cual se regula con amplitud, dada la heterogeneidad existente en esta materia en los diversos Estados miembros. La autoridad que valide la OEE, también podrá considerarse como autoridad emisora a los efectos de la transmisión del EPOC (art. 4.4 PROGC). Valoramos positivamente este sistema de validación, dado que consideramos que está previsto para aquellos Estados en los que la policía pueda acordar directamente medidas de in-

tando el Consejo su orientación general el 7/02/2021 (nº doc. 9005/21, 28/05/2021). Tiene como finalidad, entre otras, lograr mayor eficiencia en la cooperación judicial en materia penal, con el establecimiento de un canal de comunicación seguro respecto a la transmisión de solicitudes de pruebas electrónicas. Es posible que finalmente la OEE y la OEC, se transmitan y ejecuten a través de este futuro sistema, en lugar de por los mecanismos previstos en la PROCG y la PRLIBE. También podría utilizarse la Plataforma SIRIUS de Europol, para el acceso a las pruebas electrónicas en las investigaciones penales, que permite afrontar la complejidad de la investigación en Internet y compartir experiencias entre las autoridades, véase: *https://www.europol.europa.eu/activities-services/sirius-project* (fecha de consulta: 3 de diciembre de 2021).

[43] Fuentes Soriano, O. (2020). *Op. cit.*, pág. 306, se ha cuestionado por la Abogacía Europea que no se permita a los acusados solicitar una OEE en las mismas condiciones que el Fiscal, lo cual podría ir en detrimento de la igualdad procesal. El Comité Económico y Social Europeo, considera que permitir que el Fiscal pueda emitir la OEE, conculca la normativa de protección de datos, propugnando que siempre la emita una autoridad judicial.

[44] Conforme al art. 22 PROGC, los Estados deberán comunicar a la Comisión, con la fecha límite de la aplicación del Reglamento, las autoridades que son competentes para emitir, validar, ejecutar y pronunciarse sobre las objeciones de los destinatarios del art. 16, el cual coincide en lo sustancial con el art. 22 PRC, a diferencia del art. 22 PRLIBE, donde la dicha fecha se fija en doce meses antes de la de aplicación del Reglamento.

vestigación, constituyendo una garantía al existir de esta forma siempre un control por un órgano jurisdiccional o un Fiscal, lo cual también está previsto para estos supuestos en la OEI[45], donde obviamente también se tuvo en cuenta la referida heterogeneidad en cuanto a las autoridades competentes para la investigación en los Estados miembros. Sin embargo, si la OEE va referida a datos de transacciones (de tráfico en art. 4.2 PRLIBE) y de contenido, se excluye la posibilidad que el Fiscal constituya autoridad de emisión (o validación), coincidiendo las otras autoridades y condiciones que acabamos de exponer respecto a la primera categoría de datos, si bien siempre tendrá que validar la OEE un órgano jurisdiccional (art. 4.2 PROGC)[46]. Cabría plantearse, si en los datos de transacciones y de contenido, el Fiscal podría ser autoridad de emisión, si la legislación del Estado emisor la definiera como autoridad para la investigación en procesos penales con competencia para la obtención de pruebas (conforme al art. 4.2 b) PROGC), aunque en este caso siempre será necesaria la validación por un órgano jurisdiccional.

Consideramos que la mencionada exclusión constituye un acierto, que conlleva un refuerzo de las garantías, al establecerse siempre el control judicial en esta segunda categoría de datos, ya que las medidas de investigación y actos de prueba sobre los mismos poseen un mayor carácter invasivo o coercitivo. Por otro lado, sería posible sólo respecto a los datos de abonados y de acceso, que las autoridades que requieren validación previa para la emisión de la OEE, puedan emitirla en casos urgentes sin validación, si ésta no se puede obtener a tiempo y pudieran emitir la

[45] Como destaca respecto a este instrumento, Bachmaier Winter, L. (2015). "Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la Orden Europea de Investigación". Revista General de Derecho Europeo, nº 36, págs. 7, 8, 16 y 33. Disponible en: *https://www--iustel--com.us.debiblio.com/v2/revistas/detalle_revista.asp?id_noticia=416104* (fecha de consulta: 3 de diciembre de 2021). También en este sentido, Tosza, S. (2020). *Op. cit*., pág. 171.

[46] Rogalski, M. (2020). *Op. cit*., págs. 342-345. Se diferencian estos dos grupos de categorías de datos, en función de su sensibilidad, con distintos niveles de protección, lo cual repercute en las autoridades competentes. La primera categoría es más adecuada para la identificación del investigado y la segunda, para la obtención de la prueba para el juicio oral. Respecto a que en los datos de identificación y de acceso no sea necesaria la validación por un órgano jurisdiccional, en principio, ello puede considerarse que está de conformidad con la jurisprudencia del TJUE (asuntos acumulados C-203/15 y C-698/15 *Tele2 Sverige AB v. Post-och telestyrelsen*), según la cual sería viable el control por una autoridad administrativa independiente. Propone que siempre exista un control judicial, entre otras razones, dado que el Fiscal no siempre constituye una autoridad independiente.

orden en un caso interno similar sin validación[47], supuesto en el que ésta se solicitará en el plazo máximo de 48 h. Si se denegara la validación posterior, la autoridad emisora retirará la orden, suprimiendo los datos o garantizando que éstos no se utilicen como prueba (art. 4.5 PROGC, única versión que contempla los casos de urgencia).

3. Garantías, condiciones para la emisión y vías de recurso

El sistema de garantías continúa desarrollándose en las condiciones para su emisión. Se establece expresamente la vigencia de los principios de necesidad y proporcionalidad[48], que únicamente podrá emitirse la OEE en el ámbito de los procesos penales y si en el Estado emisor está

[47] Carrera, S., Stefan M. y Mitsilegas, V. (2020). Cross-border data Access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic. Report of CEPS and QMUL Task Force, Centre for European Policy Studies, Bruselas, págs. 49 y 57-58. Disponible en: *https://www.ceps.eu/download/publication/?id=30689&pdf=TFR-Cross-Border-Data-Access.pdf* (fecha de consulta: 3 de diciembre de 2021). Si bien conforme a la jurisprudencia del TJUE es necesaria la revisión previa por un Órgano Jurisdiccional u organismo administrativo independiente, para el acceso a los datos solicitados, ello puede, en principio, no aplicarse sólo en los casos de "urgencia válidamente establecida".

[48] La aplicación del principio de proporcionalidad en este instrumento debería ostentar una posición y función primordial, pudiendo constituir en gran medida el eje vertebrador de todo el sistema, del mismo modo que el principio de necesidad. La responsabilidad de garantizar el respeto de los referidos principios, corresponde a la autoridad emisora en cada caso concreto (considerandos nºs 24 y 46 PROGC). El respeto de los principios de necesidad y proporcionalidad, se propugna además en los considerandos nºs 29, 38, 43, 44, 54 y 57 PROGC, entre otros. Su aplicación se realizará de conformidad con la CDFUE (considerandos nºs 2 y 12 PROGC), del mismo modo que el respeto de los derechos fundamentales, las garantías procesales, la protección de datos y la confidencialidad. Como ya habían destacado, Cocq, C. y Galli, F. (2015). "The Use of Surveillance Technologies for the Prevention, Investigation and Prosecution of Serious Crime". EUI Working Papers, Department of Law, nº 41, pág. 48. Disponible en: *https://cadmus.eui.eu/handle/1814/37885* (fecha de consulta: 3 de diciembre de 2021), respecto al marco normativo europeo sobre la privacidad, la retención de datos afecta a los derechos fundamentales a la privacidad y a la protección de datos personales reconocidos en los arts. 7 y 8 CDFUE. Cualquier limitación o intrusión tiene que regularse de forma clara y predecible, proporcional y necesaria (art. 52.1 CDFUE). Considera Robinson, G. (2018). *Op. cit*., págs. 350-351, que las garantías procesales y la aplicación de los principios de proporcionalidad y necesidad, debe realizarse conforme a la jurisprudencia en materia de retención y protección de datos para investigaciones penales del TJUE (asuntos *Digital Rights Ireland* y *Tele2 Sverige*), además de respetar el RGPD. También sobre los derechos fundamentales y los referidos principios, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) y del TJUE, véase Daniele, M. (2019). *Op. cit*., págs. 1284-1285.

prevista una medida similar para la misma infracción penal en una situación interna equiparable[49], lo cual observamos que evita el *forum shoping* probatorio, dada la ausencia de armonización[50] en materia de admisibilidad probatoria en el ámbito europeo, además de poner de manifiesto la relevancia de la *lex fori* e incluso, constituye una forma de garantizar la posterior admisibilidad probatoria (art. 5.2 PROGC y PRLIBE, versión que desarrolla con detalle estas garantías). Además de la relevancia y vigencia de los mencionados principios, constituye un refuerzo de las garantías la restricción de su ámbito de aplicación a los procesos penales, a diferencia de la OEI[51], donde fue cuestionado que se permita para procesos de naturaleza diferente, del mismo modo que sólo se permita cuando esté prevista en el Estado de emisión una medida similar, en los términos expuestos, ya que ello impediría que la OEE se utilizara para la obtención de pruebas que no estuvieran permitidas según la *lex fori*.

La aplicación del principio de proporcionalidad se refleja en las condiciones para la emisión referidas a los tipos de infracciones penales y a los límites penológicos *a quo*[52] de la OEE. Hay que diferenciar por un

---

[49] Geraci, R. M. (2019). *Op. cit.*, pág. 1345. Esta previsión refleja la "cláusula de cortesía internacional", que del mismo modo que los principios de necesidad y proporcionalidad, se contempla en instrumentos de cooperación judicial de "última generación", como la OEI.

[50] Carrera, S., Stefan M. y Mitsilegas, V. (2020). *Op. cit.*, pág. 59. Existe un alto nivel de fragmentación entre los sistemas de justicia penal, una "persistente" ausencia de armonización en la normativa sobre admisibilidad de pruebas penales y una aplicación "inconsistente" del acervo sobre los derechos procesales.

[51] Tosza, S. (2020). *Op. cit.*, pág. 71. La OEE posee un ámbito de aplicación más estrecho que la OEI.

[52] La aplicación de este principio estimamos que requiere una regulación detallada con límites penológicos y requisitos específicos, para que no constituya un concepto jurídico indeterminado. Harbo, T. I. (2017). "Introducing procedural proportionality review in European Law". Leiden Journal of International Law, vol. 30, nº 1, págs. 26-27, 32, observa que la revisión de la proporcionalidad genera un espacio para la discreción judicial, proponiendo un concepto de revisión procesal de la proporcionalidad como alternativa a la revisión convencional, según la cual los órganos jurisdiccionales comprobarán si se han tenido en cuenta consideraciones irrelevantes, si la medida es arbitraria, discriminatoria o manifiestamente irrazonable ("revisión de las cuatro esquinas"). Además, Herlin-Karnell, E. (2019). The constitutional structure of Europe´s Area of ´Freedom, Security and Justice´ and the right to justification. Hart Publishing, Oxford, págs. 64-65, destaca que el concepto de proporcionalidad se vuelve aún más complejo en el ELSJ, dada la necesidad de evitar que los instrumentos de reconocimiento mutuo se utilicen para delitos menores y por la necesidad de combinar la eficacia con la protección de los derechos. Las críticas a la proporcionalidad, se centran en su interpretación como principio, constituyendo un concepto demasiado vago que indirectamente erosiona los derechos humanos. Resalta que en el ELSJ donde la seguridad posee una posición dominante, parece haber-

lado la OEE referida a datos de abonados o de acceso, dado que en estos supuestos puede emitirse respecto a todas las infracciones penales[53], si bien respecto a estas categorías de datos, si se tratara de la ejecución de una pena o medida de seguridad privativa de libertad, ésta deberá tener una duración mínima de cuatro meses (art. 5.3 PROGC). Por tanto, en dichas categorías de datos, existen menores restricciones que respecto a los datos de transacciones o de contenido, ya que, en éstos al conllevar una injerencia superior en los derechos fundamentales, se requiere que la OEE se emita respecto a infracciones penales con un límite penológico *a quo* de tres años de privación de libertad en el Estado de emisión (art. 5.4 a) PROGC) o bien se restringe a determinadas infracciones penales[54], combinándose los criterios cuantitativo y cualitativo[55] en la determina-

se excluido la inicial concepción europea del principio de proporcionalidad. Nosotros observamos, que dicho margen de discreción judicial, puede presentar el riesgo de que la proporcionalidad se aplique en virtud de criterios de oportunidad, lo cual iría en detrimento de las garantías.

[53] Stefan, M. y G. González Fuster, G. (2018). *Op. cit.*, págs. 35-36. Es problemático que no se determinen de forma precisa los delitos en esta categoría de datos en el art. 5 PRC, ya que no existe una comprobación de la legalidad, necesidad y proporcionalidad por las autoridades judiciales del Estado de ejecución. En este sentido, Gialuz, M. y Della Torre, J. (2018). *Op. cit*., págs. 293-295, objetan que no se establezca ningún límite en dicha categoría de datos y que los únicos parámetros de la "necesidad" y "proporcionalidad" pueden ser vagos e insuficientes. El propósito de crear un instrumento fuertemente garantista, puede que no se consiga. Parece que la UE está priorizando la seguridad, sin prestar suficiente atención a las garantías, no debiéndose olvidar la libertad y la justicia. Destacamos que la postura de la Comisión LIBE, precisamente intenta elevar dicho nivel de garantías.

[54] El establecimiento de un límite penológico *a quo* respecto al acceso a los datos, es una cuestión relevante en la aplicación de la proporcionalidad. Así se refleja en la Sentencia del TJUE (Gran Sala), 2/10/2018, asunto C-207/16, cuestión prejudicial planteada por la Audiencia Provincial de Tarragona. En las conclusiones del Abogado General se diferencia entre el acceso a los datos de identificación y los datos de tráfico, localización y comunicaciones, observándose respecto a la gravedad del delito y el principio de proporcionalidad, que es imposible determinarlo sólo por la penalidad abstracta, dadas las diferencias existentes en los Estados miembros. Por ello observamos que la propuesta de Reglamento generaría el beneficio de esclarecer este extremo, coadyuvando a la seguridad jurídica con dicho límite penológico *a quo* y la restricción a determinadas infracciones.

[55] Rogalski, M. (2020). *Op. cit.*, págs. 346-348. No se resuelve el problema de que el mismo delito tenga señaladas penas de distinta duración en los Estados miembros cuando se aplique el criterio cuantitativo, a diferencia del grupo de delitos armonizados en la UE (criterio cualitativo). Ello generaría la situación de que, en un mismo tipo de proceso penal, se puedan obtener y admitir pruebas que no se puedan obtener en otros Estados. Propone que se incorpore una lista de delitos, como la que existe en otros instrumentos, lista de treinta y dos delitos donde no se efectúa el control de la doble tipificación. Recordemos que, en la PRLIBE, sí se incorpora dicha lista.

ción de los límites conforme al principio de proporcionalidad[56], lo cual se refleja además en las diferentes autoridades de emisión.

El criterio cualitativo conlleva que el referido límite penológico no se aplicará, cuando la OEE vaya referida a los datos de transacciones o de contenido, en una serie específica de infracciones penales, si éstas se hubieran cometido total o parcialmente a través de un sistema de información (art. 5.4 b) PROGC)[57]. Tampoco se aplica dicho límite penológico ni se requiere que las infracciones se hayan cometido a través de un sistema de información, si se tratara de delitos de terrorismo, delitos relacionados con un grupo terrorista, con actividades terroristas y la complicidad, inducción y tentativa respecto a los mismos (art. 5.4 c) PROGC)[58]. El criterio cualitativo permite la obtención de los datos, en determinadas infracciones donde la prueba electrónica es en todo caso relevante e incluso la modalidad predominante. De todos modos, en los datos de transacciones o de contenido, siempre estará vigente el límite de cuatro

[56] Danielle, M. (2019). *Op. cit.*, págs. 1285-1287, califica como un sistema de "geometría variable" las diferencias en los requisitos de la OEE en función de las categorías de datos. Opina que el limite penológico *a quo* de tres años de la segunda categoría de datos, constituye un límite bajo que puede "anular" la diferencia entre las órdenes menos o más invasivas, justificando que no exista el tradicional control de la doble tipificación existente en la OEI, en que podría ser inaplicable, dada la multiplicación de la *lex loci*. Gialuz, M. y Della Torre, J. (2018). *Op. cit.*, pág. 285, justifican la exclusión de dicho control, en el alto nivel de confianza en el respeto de los derechos fundamentales por los Estados miembros. En cuanto a la aplicación de la proporcionalidad y necesidad, observan que la iniciativa normativa no aclara de forma expresa al Estado emisor, el estándar probatorio para la emisión de las órdenes. Tosza, S. (2020). *Op. cit.*, pág. 178, destaca que la OEE requiere un nivel de confianza mutua superior al de los clásicos instrumentos de reconocimiento mutuo, como se refleja en la exclusión del referido control de la doble tipificación, estando previstos menos motivos de denegación que en la OEI.

[57] Se trata de las infracciones penales contempladas en los artículos 3 a 5 de la Decisión Marco 2001/413/JAI del Consejo, por tanto, de los delitos relacionados con equipos informáticos, dispositivos especialmente adaptados y la participación, instigación y tentativa en relación a los mismos. También de las infracciones penales descritas en los artículos 3 a 7 de la Directiva 2011/93/UE, consistentes en infracciones relacionadas con los abusos sexuales, explotación sexual, pornografía infantil, embaucamiento de menores con fines sexuales por medios tecnológicos y la inducción, complicidad y tentativa con los anteriores. En estas últimas, en la PRLIBE no se requiere que se hayan cometido total o parcialmente a través de un sistema de información (art. 4 bis, b bis)). Además, de las infracciones definidas en los artículos 3 a 8 de la Directiva 2013/40/UE, referidas al acceso e interferencia ilegal a los sistemas de información, interferencia e interceptación ilegal en los datos informáticos, a los instrumentos utilizados para cometer las infracciones y la inducción, complicidad y tentativa.

[58] Infracciones contempladas en los artículos 3 a 12 y 14 de la Directiva (UE) 2017/541.

meses para la ejecución de una pena o medida de seguridad privativa de libertad (art. 5.4 d) PROGC).

Conforme al principio de especialidad, las pruebas electrónicas no podrán utilizarse en un procedimiento distinto a aquel en el que se obtuvieron, salvo que se pudiese haber emitido la OEE conforme al art. 5.3 y .4 que acabamos de tratar o bien, para evitar una grave e inmediata amenaza para la seguridad pública o los intereses fundamentales el Estado emisor[59], supuestos en los que también se permitiría que las pruebas electrónicas se transmitan a otro Estado miembro (art. 12 ter.1 y .2 PROGC, única versión que contempla este principio). Respecto a este último supuesto, estimamos que la aplicación del principio de proporcionalidad debería ser prioritaria, dado que no está delimitado con un límite penológico *a quo* específico y la referencia a los "intereses fundamentales" del Estado emisor, puede tener límites demasiado imprecisos, con el riesgo de que se utilicen los datos obtenidos con la OEE en otro proceso diferente donde no se verificaran los referidos requisitos del art. 5.3 y .4 y, la autoridad judicial no actuó como autoridad emisora, por lo que no se pudieron hacer valer en ese proceso en concreto, las garantías previstas para la emisión y ejecución de la OEE. Por otro lado, sería posible la transferencia de las pruebas electrónicas obtenidas a un tercer Estado o a una organización internacional, si concurren las mismas situaciones que en los supuestos anteriores y las condiciones para la transferencia de datos personales a terceros países[60] u organizaciones internacionales, según el Capítulo V de la Directiva (UE) 2016/680, de protección de datos.

La tutela judicial efectiva se garantiza con el reconocimiento del derecho al recurso ante un órgano jurisdiccional[61] del Estado emisor de la OEE conforme a su legislación nacional (art. 17 PROGC). La autoridad emisora deberá garantizar que se informe sobre las vías de recurso efectivas[62], las

[59] En el art. 11 bis PRLIBE la utilización de la información electrónica en otros procedimientos, se restringe a las situaciones en las que exista una amenaza inminente para la vida o integridad física de otra persona.

[60] Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit*., pág. 53, destacan la sentencia de 2020 del TJUE en el asunto *Schrems II*, según la cual el desarrollo de nuevos instrumentos de cooperación internacional que permitan el acceso a los datos en la UE por terceros países que no cumplan los estándares de protección de datos de la UE, sería imposible sin la participación de las autoridades de supervisión de la UE.

[61] Geraci, R. M. (2019). *Op. cit*., págs. 1353-1355. El derecho al recurso se reconoce de conformidad con el art. 47 CDFUE. Destacamos que el derecho al recurso permitiría que, si la autoridad emisora no es un órgano jurisdiccional, se reconduzca la OEE a dicho órgano a través de este cauce.

[62] Tosza, S. (2020). *Op. cit*., pág. 178. Es cuestionable que se pueda hablar de vías de recurso efectivas, cuando una persona pueda ser investigada en otro Estado miembro,

cuales tendrán los mismos plazos y condiciones que en casos internos similares, garantizándose el ejercicio efectivo del recurso. La persona cuyos datos se soliciten a través de una OEE (tanto si se trata del investigado o acusado como de otra persona diferente cuyos datos se hayan obtenido), podrá impugnar en el Estado emisor la legalidad, necesidad y proporcionalidad de la medida. Por ello, sin perjuicio de otras vías de recurso previstas en el ordenamiento del Estado emisor, las personas cuyos datos se soliciten tendrán derecho a vías de recurso efectivas contra la OEE. En el caso de los investigados o acusados, éstos podrán utilizar las vías de recurso durante el proceso penal en el que se utilicen los datos[63]. Esta previsión respecto al derecho al recurso, se establece sin perjuicio de las que existan conforme a referida la Directiva (UE) 2016/680 y el RGPD. Vemos, por tanto, como al margen de las previstas en estos instrumentos normativos europeos, las vías de recurso dependerán del ordenamiento de cada Estado emisor, estableciéndose la que podríamos considerar como una "obligación de mínimos", pudiendo existir obviamente diversos sistemas de recursos en virtud de los distintos estándares de garantías internas. Además, se establece la obligación de que en los procesos penales en el Estado emisor, se respeten los derechos de defensa y equidad en la valoración de las pruebas obtenidas, conforme a la tutela judicial efectiva[64].

4. Contenido

La información o contenido que incluirá la OEE, consiste en la autoridad emisora y validadora (si existiera), el destinatario, el usuario, salvo que la única finalidad sea la de identificarlo o bien, cualquier otro identifi-

---

en otra lengua y desconociendo la transferencia de los datos. Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit.*, pág. 59, argumentan que la falta de participación significativa de las autoridades de supervisión en los Estados de ejecución, repercute en la seguridad jurídica, limitándose el derecho a un recurso efectivo que se reconoce en el Derecho de la UE.

[63] Gómez Amigo, L. (2019). *Op. cit.*, pág. 50. En realidad, en este supuesto lo que se contempla es la impugnación de la incorporación de la prueba obtenida al proceso penal. Estamos de acuerdo con ello, respecto a los investigados o acusados, que tendrán derecho al recurso en el proceso penal donde se utilicen los datos. Por tanto, se contemplan dos previsiones, una respecto al investigado o acusado y otra de carácter más general, referente a cualquier persona cuyos datos hayan sido solicitados (*v. gr.* terceros procesales).

[64] En el art. 17 PRLIBE, a diferencia de las otras versiones, se innovan las vías de recurso, también se prevén respecto a la OEC y se contempla que el recurso pueda interponerse tanto ante un órgano jurisdiccional del Estado emisor (motivos de fondo) como en el Estado de ejecución (garantías de los derechos fundamentales).

cador único (nombre de usuario, identificador o nombre de la cuenta), la categoría de los datos solicitados, el período que comprende la solicitud de entrega, la *lex fori* de naturaleza penal, las razones que justifiquen que se trata de un caso urgente o petición de revelación rápida de la información y la justificación de la necesidad y proporcionalidad de la medida (art. 5.5 PROGC). Existen previsiones específicas para el supuesto de que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa o entidad distinta de la persona física, supuesto en que la OEE sólo podrá remitirse al proveedor de servicios si no son apropiadas otras medidas, si pudiera ponerse en riesgo la investigación (art. 5.6 PROGC)[65]. El EPOC deberá contener toda esta información, junto con los datos que permitan al destinatario identificar y contactar con la autoridad emisora, salvo la justificación de la necesidad y proporcionalidad y cualquier otra precisión adicional sobre las investigaciones (art. 8.3 PROGC), dado que el destinatario es el proveedor de servicios y no una autoridad, lo cual justifica estas omisiones en el EPOC.

En el supuesto de que la orden está referida a datos de transacciones y la autoridad emisora tenga razones fundadas por las que considere que la persona respecto a la que se solicitan los datos no reside en el Estado emisor, dicha autoridad deberá solicitar aclaraciones, efectuando las oportunas consultas (art. 5.7 a) PROGC). Además, si los datos de transacciones están protegidos por privilegios o inmunidades según la Ley del Estado de ejecución o están sometidos a normas sobre la determinación y limitación de responsabilidad respecto a la libertad de prensa y de expresión, o si la revelación de su contenido pudiera repercutir en intereses del Estado de ejecución como la seguridad y defensa nacionales, la autoridad emisora pedirá aclaraciones sobre estas situaciones[66]. Si la autoridad emisora considera que concurren dichas situaciones, las tendrá en cuenta al igual que si se contemplaran en su Derecho interno, pudiendo no emitir o adaptar la OEE, o solicitar la retirada del privilegio o inmunidad[67] a la autoridad

[65] En el art. 5.6 bis PROGC se añade un supuesto que no existe en las otras versiones, consistente en que, si la OEE va referida a datos integrantes de una infraestructura que el proveedor de servicios preste a una autoridad pública, sólo podrá emitirse la OEE si esta autoridad se encuentra en el Estado emisor.

[66] Fuentes Soriano, O. (2020). *Op. cit.*, pág. 315. Este tratamiento sobre informaciones que pueden ser especialmente sensibles en la legislación de un Estado específico, refleja la finalidad de salvaguardar los derechos fundamentales conforme a la CDFUE y las particularidades normativas internas de cada Estado miembro.

[67] La posibilidad de que se adapte la OEE o se solicite la retirada del privilegio o inmunidad, sólo se contempla en la PROGC. En el art. 5.7 PRC y PRLIBE, sólo se prevé la opción de no emitir la OEE.

competente (arts. 5.7 b), .8 y 7 bis.3 PROGC). La autoridad notificada[68] (del Estado de ejecución), podrá informar a la mayor brevedad de cualquiera de estas circunstancias en el plazo máximo de diez días y si la autoridad de emisión optara por retirar la orden, lo notificará al destinatario (art. 7 bis.2 PROGC). Estas notificaciones carecen de efecto suspensivo en lo referente a las obligaciones del destinatario de las mismas (art. 7 bis.4 PROGC). Estos supuestos pueden generar una restricción sobre el uso de los datos obtenidos conforme al art. 12 bis PROGC, que respecto a los datos de transacciones o de contenido, regula la actuación de la autoridad emisora, *mutatis mutandis* en términos similares a los que acabamos de exponer.

5. Ejecución

La OEE se remitirá directamente al representante legal que haya designado el proveedor de servicios a efectos de recabar pruebas para procesos penales, salvo que el mismo no haya sido designado, supuesto en el que se podrá remitir a cualquier establecimiento en la UE de dicho proveedor (art. 7.1 y 7.2 PROGC). También se aplicará esta solución, si el representante legal no ejecutara el EPOC en un caso urgente conforme al art. 9.2 PROGC (art. 7.3 PROGC) y si el representante no cumpliera con las obligaciones que le corresponden conforme a los arts. 9 y 10 y la autoridad emisora estimara que concurre un grave riesgo de pérdida de datos[69].

Tras la recepción del EPOC, el destinatario transmitirá los datos requeridos de forma directa a la autoridad emisora o a las autoridades indicadas en el EPOC en un plazo máximo de diez días, salvo que la autoridad emisora requiera una mayor rapidez indicando las razones, transmisión que se tendrá que efectuar a través de un medio seguro fiable que garantice la autenticidad e integridad. En casos urgentes[70], la remisión tendrá

[68] Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit*, págs. 49 y 57. Con carácter general la principal enmienda propuesta por el Consejo respecto a la PRC, consiste en la introducción de un sistema de notificaciones a las autoridades del Estado de ejecución en aspectos sensibles como los referidos.

[69] En la PRLIBE, se establece la innovación de que la OEE se remitirá "directa y simultáneamente", al establecimiento principal del proveedor de servicios o en su caso al representante legal en el Estado de ejecución y a la autoridad de ejecución (arts. 7.1, 8 bis.1 y 9.1 bis), que podrá ser una autoridad judicial (art. 2.14)). Consideramos que esta innovación es claramente más garantista y que facilitaría la posterior admisión probatoria.

[70] Estos se definen conforme al art. 2.15) PROGC, como aquellos donde concurra una "amenaza inminente" para la vida o integridad física de una persona, o bien para una

lugar en el plazo máximo de seis horas desde la recepción del EPOC (art. 9.1 y 9.2 PROGC)[71]. Este último plazo, como vimos, se incrementa a dieciséis horas en la PRLIBE (arts. 8 bis.3 y 9.1 bis). La remisión directa y ejecución por el representante legal (o proveedor de servicios) y la limitación de la intervención de la autoridad del Estado de ejecución a supuestos puntuales, aspectos que hemos destacado, junto con los plazos tan reducidos para la ejecución, podría afectar a las garantías procesales[72], lo cual repercutiría en la posterior validez y admisibilidad de la prueba obtenida. Por ello consideramos que, aunque este instrumento presente indudables ventajas en la obtención de la prueba, es necesario que existan mecanismos para preservar las garantías y los derechos, entre otras razones, para evitar que finalmente la prueba devenga inválida.

El proveedor de servicios podrá reclamar al Estado emisor el reembolso de los gastos incurridos, siempre que ello esté previsto en la legislación de dicho Estado respecto a las órdenes nacionales que se emitan en situaciones similares (art. 12 PROGC). Sin embargo, en el art. 12 PRLIBE sí se establece la obligación de reembolso de gastos por el Estado emisor siempre que el proveedor de servicios lo solicite, pudiéndolo solicitar por razones prácticas al Estado de ejecución, al cual reembolsará posteriormente el Estado emisor[73].

---

infraestructura esencial, definida en el art. 2.a) de la Directiva 2008/114/CE del Consejo, sobre infraestructuras críticas europeas y su protección.

[71] Rogalski, M. (2020). *Op. cit*., págs. 350-352. Estos plazos tan breves, en los que los proveedores o sus representantes deberán verificar los requisitos de forma y fondo de la OEE, pueden conllevar que prioricen la OEE en lugar de las solicitudes de las autoridades de su propio país.

[72] Daniele, M. (2019). *Op. cit*., págs. 1288-1293. El aspecto más preocupante estriba en confiar a los proveedores de servicios el control sobre la ejecución, lo cual supone la "privatización de la tutela de los derechos fundamentales". Ello no constituye una particularidad de esta Propuesta, existiendo un mecanismo similar en la *U.S. Cloud Act*, por lo que estaríamos ante una tendencia que se está imponiendo a nivel global. Propone como solución crear un órgano jurisdiccional europeo para realizar los controles que se encomiendan a los proveedores. Estimamos que estos problemas se solventarían con la posición de la PRLIBE, donde las órdenes también se remiten a una autoridad del Estado de ejecución. Además, Mitsilegas, V. (2018). *Op. cit*., pág. 265, que igualmente alerta de dichos riesgos y que la propuesta de Reglamento está en consonancia con la *U.S. Cloud Act*, creándose una "convergencia transatlántica" que privilegia la eficacia en la investigación sobre la protección de los derechos.

[73] Esta solución estimamos que es más operativa y facilita la ejecución. Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit*., pág. 60. Es importante que se incorpore una información armonizada sobre el reembolso, los proveedores están preocupados por tener que afrontar los gastos de elevados volúmenes de órdenes y solicitar el reembolso en el Estado de emisión, distinto a aquél donde prestan u ofrecen sus servicios.

Para las incidencias que puedan surgir durante la ejecución, está previsto el formulario del Anexo III. De este modo, si el destinatario no puede ejecutar el EPOC porque esté incompleto, posea errores manifiestos o carezca de la información suficiente, lo comunicará a la mayor brevedad a la autoridad emisora solicitándole las aclaraciones necesarias a través de dicho formulario, informándole igualmente respecto a si fuera posible la identificación y conservación de los datos. La autoridad emisora responderá en el plazo máximo de cinco días, suspendiéndose los indicados plazos de transmisión de datos, hasta que no proporcione al destinatario las aclaraciones requeridas (art 9.3 PROGC). También el destinatario informará con inmediatez a la autoridad emisora a través del Anexo III, si le resultara imposible cumplir con sus obligaciones por circunstancias no creadas por él o por el proveedor de servicios al recibir la orden, explicando las razones (art. 9.4 PROGC)[74]. Si fueran otros los motivos por los que el destinatario del EPOC no aportara los datos solicitados, no facilite detalladamente la información o en plazo, también tendrá que informar a la autoridad emisora inmediatamente y dentro de los plazos de transmisión referidos, a través del Anexo III, tras lo cual la autoridad emisora, podrá fijar un nuevo plazo para la entrega (art. 9.6 PROGC). No obstante, el destinatario deberá conservar los datos si no los entregara con inmediatez, salvo que con la información del EPOC no pueda identificarlos, hasta que los entregue conforme a la OEE y su certificado o bien a través de otros cauces como la asistencia judicial mutua. Si la entrega y conservación de datos ya no fueran necesarias, la autoridad emisora y cuando proceda la de ejecución, informarán inmediatamente al destinatario (art. 9.7 PROGC).

Se establece la obligación de confidencialidad con la finalidad de no obstaculizar el proceso penal, la cual tendrá que respetar tanto el destinatario del EPOC como el proveedor de servicios, que no podrán informar ni del EPOC ni de los datos entregados a la persona cuyos datos se solicitan, salvo que expresamente así lo pida la autoridad emisora, supuesto en el que ésta incorporará la información sobre las vías de recurso disponibles (art. 11.1 PROGC). En el supuesto de que la autoridad emisora no solicitara que se informe al titular de los datos que se solicitan, será la propia autoridad emisora a quien le corresponda informarle, pudiendo demorar dicha información al titular, con la finalidad de no obstaculizar el proceso penal (por ejemplo, para preservar el secreto sumarial), respetando los principios de necesidad y proporcionalidad (art. 11.2 PROGC).

[74] En la PROGC, se ha suprimido la posibilidad de que en este supuesto se retire el EPOC, lo cual se establece en el art. 9.4 *in fine* PRC, además del supuesto previsto en el art. 9.5,2 PRC, como hemos visto.

Precisamente estos principios también deberán fundamentar la decisión de la autoridad emisora de abstenerse de informar a la persona titular de los datos solicitados, con la finalidad de proteger los derechos fundamentales e intereses legítimos de otra persona, sobre todo si prevalecen sobre el interés de información del titular de los datos (art. 11.3 PROGC)[75].

Si el destinatario no ejecutara el EPOC en el plazo establecido y sin indicar razones que acepte la autoridad emisora, ésta podrá trasladar a la autoridad competente del Estado de ejecución la OEE con el EPOC y el Anexo III que, en su caso, el destinatario hubiera remitido y, cualquier otro documento pertinente, para que dicha autoridad proceda a la ejecución (art. 14.1 PROGC). Es éste el supuesto en el que se prevé la remisión a una autoridad del Estado de ejecución en las versiones del Reglamento, donde con carácter general la OEE se remitirá únicamente al representante designado por el proveedor de servicios, a diferencia de lo establecido en la PRLIBE, según la cual como vimos, siempre se remite simultáneamente la OEE a la autoridad de ejecución[76]. Tras la recepción por la autoridad de ejecución de la documentación, reconocerá la OEE sin demoras indebidas y en el plazo máximo de cinco días hábiles, adoptando las medidas para la ejecución, salvo que considere que concurren algunos de los motivos de denegación del art. 14.4 PROGC (art. 14.2 PROGC). Por otro lado, si los datos solicitados estuvieran protegidos por privilegios o inmunidades, se actuará conforme a las previsiones del art. 5.8, expuestas *ut supra* (arts. 14.2 bis y 14.4 f) PROGC).

La autoridad de ejecución cuando reconozca la OEE, requerirá al destinatario para que la cumpla informándole del plazo para ello y de que podrá oponerse a la ejecución conforme a los motivos del art. 14.4 a) a e), del mismo modo que del sistema sancionador en caso de incumplimiento (art. 14.3 PROGC). Si el destinatario se opusiera, la autoridad de ejecución decidirá sobre la ejecución de la OEE con la base de la información que éste le proporcione y la información adicional transmitida por la autoridad emisora, a la cual consultará antes de la decisión que adopte

[75] En el art. 11 PRLIBE, con una orientación más garantista, se establece que el proveedor de servicios informará sin demora al titular de los datos solicitados. Sólo se prevé la omisión de esta información, si la autoridad emisora lo solicita expresamente al proveedor de servicios, dictando al efecto una resolución judicial que revisará periódicamente, con la duración de la confidencialidad conforme a los principios de necesidad y proporcionalidad.

[76] De hecho, en el art. 14.1 PRLIBE se contempla la falta de cumplimiento del EPOC en otros términos, dado que para que la autoridad emisora pueda solicitar a la del Estado de ejecución que ejecute la OEE, se requiere que el proveedor de servicios no cumpla con el mismo sin aportar razones y que la autoridad de ejecución no invocara los motivos de denegación del reconocimiento o de la ejecución previstos en el art. 10 bis PRLIBE.

sobre el reconocimiento o ejecución (art. 14.6 y .7 PROGC). La autoridad de ejecución cuando obtenga los datos, los transmitirá a la autoridad emisora en el plazo de dos días hábiles, salvo que éstos estén protegidos por privilegios, inmunidades, normas sobre limitación de responsabilidad penal respecto a la libertad de prensa y de expresión, o afecten a intereses fundamentales como la seguridad y defensa nacionales, supuestos en los que se podrán no transmitir los datos (art. 14.9 PROGC)[77]. Si el destinatario incumpliera con una orden confirmada por la autoridad de ejecución, ésta podrá imponer una sanción pecuniaria conforme a su legislación nacional, contra la cual se prevé un recurso efectivo (art. 14.10 PROGC)[78]. Los motivos de denegación del reconocimiento o ejecución de la OEE, se establecen de forma tasada en el art. 14.4 PROGC[79], siendo tanto de forma como de fondo. Se trata de que la OEE no se haya emitido o validado por la autoridad emisora, que no se cumplan los requisitos de las infracciones penales respecto a las que se puede emitir conforme al art. 5.4 PROGC, que el EPOC no se pueda ejecutar por imposibilidad material o porque contenga errores manifiestos, que en el momento de la recepción del EPOC los datos no estén almacenados por el proveedor de servicios o bien en su nombre, que se trate de un servicio no cubierto por el Reglamento y finalmente, que se trate de datos con las restricciones contempladas en el art. 12 bis.1 PROGC[80].

---

[77] Respecto a estos supuestos, extrapolamos lo expuesto *ut supra*, respecto a los arts. 5.7 y .8 y 12 bis.

[78] Robinson, G. (2018). *Op. cit.*, pág. 350. Está por comprobar cómo los proveedores de servicios sopesarán los múltiples intereses que están en competencia y los deberes legales para cumplir con su función en la práctica, lo cual dependerá de la transparencia del procedimiento.

[79] Gómez Amigo, L. (2019). *Op. cit.*, págs. 45-46, la falta de legalidad, necesidad y proporcionalidad de la OEE, no constituyen motivos de denegación, dado que sólo se pueden hacer valer a través de recurso en el Estado emisor, el cual sólo está previsto para la OEE. Los motivos de denegación se pueden apreciar de oficio por la autoridad de ejecución o bien, alegarse por el destinatario de la OEE, coincidiendo en gran medida con los que los proveedores pueden alegar para justificar el incumplimiento, conforme al art. 9 PRC.

[80] Esta última previsión constituye una innovación de la PROGC respecto al art. 14.4 PRC, donde se contemplaba que el EPOC fuera contrario a la CDFUE o manifiestamente abusivo, supuestos que como vimos se han suprimido y sustituido por la incorporación de los motivos del art. 12 bis.1 PROGC. También se ha suprimido la fuerza mayor como causa de no ejecución del EPOC (art. 14.4 c) PRC). En la PRLIBE se innovan significativamente los motivos de denegación, los cuales se regulan en un precepto específico, el art. 10 bis, en el cual se contemplan en lo sustancial los motivos del art. 14 PRC y además se incorporan otros adicionales, incluyéndose la lista de treinta y dos delitos en los que no se efectuará el control de la doble tipificación (Anexo III bis).

Para garantizar la efectividad de estos instrumentos, se establece un sistema sancionador[81] respecto al incumplimiento de las obligaciones de ejecución por el destinatario del EPOC y de la obligación de confidencialidad que acabamos de tratar, en virtud del cual los Estados miembros regularán las sanciones pecuniarias que se puedan imponer al proveedor de servicios, las cuales deberán ser eficaces, proporcionadas y disuasorias, del mismo modo que implementarán las medidas necesarias para garantizar que se dichas sanciones se apliquen[82]. El límite *ad quem* de dichas sanciones, se establece en el dos por ciento del total del volumen anual de negocios mundial del ejercicio precedente del proveedor de servicios[83]. Este sistema sancionador está previsto con independencia de lo establecido en las legislaciones nacionales respecto a la imposición de sanciones penales (art. 13 PROGC)[84].

Están previstas otras posibles incidencias, que se contemplan bajo la rúbrica de "reexamen en caso de obligaciones contradictorias" (art. 16 PROGC)[85]. Se trata del supuesto de que el destinatario considere que

---

[81] Mitsilegas, V. (2018). *Op. cit.*, págs. 264-265. Los proveedores de servicios no están en situación de igualdad con las autoridades públicas en materia de cooperación, lo cual se evidencia en el sistema sancionador al que están sometidos, pudiéndose dificultar el control del EPOC por el riesgo de la sanción por incumplimiento.

[82] Stefan, M. y G. González Fuster, G. (2018). *Op. cit.*, págs. 34-35. Se han expresado dudas por el Comité Meijers en 2018, sobre la suficiencia de la base jurídica del artículo 13 PRC, por el que los Estados establecen el sistema sancionador, dado que el posible efecto armonizador requiere una base jurídica adicional.

[83] Bueno de Mata, F. (2021). *Op. cit.*, pág. 41. Este porcentaje de la sanción sería proporcional y oportuno, ya que lo habitual es que se traten de grandes compañías de telecomunicaciones. Existen opiniones diferentes, como Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit.*, pág. 60, que consideran que, si el importe de las sanciones es demasiado elevado, podría conllevar que los proveedores ejecuten las órdenes incluso cuando no debieran hacerlo. También, Tosza, S. (2020). *Op. cit.*, pág. 175, que opina que esta sanción podría imponerse, por ejemplo, en el caso de no proporcionar datos de una cuenta de correo electrónico, lo cual no sería proporcional, suponiendo a los grandes proveedores enormes cantidades. Por otro lado, observa que el proveedor actúa con una lógica diferente a la de las autoridades, estando motivados por sus objetivos de rentabilidad, pudiendo responder negativamente a las solicitudes de prueba electrónica si fuera más rentable que cumplirlas (pág. 178).

[84] El referido límite *ad quem*, constituye una innovación del art. 13 PROGC, que no se especifica en la PRC y en la PRLIBE, añadiéndose que los proveedores no serán responsables por el cumplimiento del EPOC.

[85] A diferencia de la PRC donde el procedimiento de reexamen se trata en dos preceptos en función de sus causas (arts. 15 y 16), en la PROGC se ha unificado la regulación en un único precepto, suprimiéndose la intervención de las autoridades centrales de los Estados y estableciéndose un tratamiento procesal más homogéneo, lo cual constituye una mejora de la regulación. Análogamente, en el art. 14 bis PRLIBE se contempla el

la ejecución de la OEE entre en conflicto con la legislación de un tercer Estado, respecto al que tendrá que informar con detalle y sin demoras, a través del Anexo III, en el plazo máximo de diez días desde la recepción del EPOC, con la consiguiente obligación de conservar los datos, lo cual del mismo modo que las anteriores incidencias expuestas, puede ralentizar notoriamente la entrega. La motivación de la objeción no podrá fundamentarse simplemente, en que en la legislación del tercer Estado no concurran análogas disposiciones sobre la emisión de una OEE, ni en que los datos estén almacenados en un tercer Estado[86]. Tras ello la autoridad emisora examinará la OEE con base en la objeción alegada, pudiendo confirmar la OEE, supuesto en el que tendrá que solicitar una revisión por el órgano jurisdiccional competente, suspendiéndose la ejecución hasta que finalice el procedimiento de revisión[87]. Observamos que ello permite que cuando la autoridad emisora no sea un órgano jurisdiccional se pueda reconducir la OEE al mismo a través de este cauce, del mismo modo que en las vías de recurso que hemos tratado en el sistema de garantías. Si este órgano concluyera que no existe un conflicto relevante confirmará la OEE y si por el contrario constatara que efectivamente la legislación del tercer Estado es aplicable y prohíbe la revelación de los datos, podrá confirmar o retirar la OEE, valorándose una serie de deter-

---

procedimiento de reexamen en un único precepto, versión donde se establece un plazo de diez días para que la autoridad de emisión decida sobre si retira, mantiene o adapta la OEE, del cual nada se dice en las otras versiones.

[86] Tosza, S. (2020). *Op. cit.*, pág. 176, ello está en consonancia con la tendencia actual, donde dado el desarrollo tecnológico, se tiende a abandonar el enfoque el principio de territorialidad tradicional. Ya que la ubicación de los datos es irrelevante en cuanto a la emisión de la OEE, ello puede provocar que los proveedores entren en conflicto con la legislación de terceros Estados, como EE.UU. De ahí la importancia de las negociaciones que la UE está efectuando con EE.UU. (pág. 170). Sobre ello, además, Carrera, S., Stefan, M. y Mitsilegas, V. (2020). *Op. cit.*, pág. 47. Conforme a la legislación estadounidense, actualmente los proveedores únicamente proporcionan voluntariamente datos sin contenido, lo cual se superaría con el nuevo marco regulador, que abarcaría otras categorías de datos, incluyendo los datos de contenido (págs. 28-35).

[87] Gómez Amigo, L. (2019). *Op. cit.*, pág. 47. Los procedimientos de reexamen serían equivalentes a la "cláusula de cortesía" de la *US Cloud Act*, por la que los proveedores de servicios norteamericanos pueden solicitar a un Tribunal estadounidense, la anulación o modificación de una orden emitida. Además, Geraci, R. M. (2019). *Op. cit.*, págs. 1353-1355 y Daniele, M. (2019). *Op. cit.*, págs. 1290-1291. Es importante la función de los proveedores en este procedimiento, ya que valorarán la existencia del conflicto legal, si bien su conducta puede condicionarse por la necesidad de mantener una buena relación con el Estado donde ejercen su actividad. Gialuz, M. y Della Torre, J. (2018). *Op. cit.*, pág. 288. Es fundamental el procedimiento de reexamen y al haberse establecido un alto nivel de garantías, se alienta a que terceros Estados establezcan un nivel de protección similar.

minados factores específicos[88]. Tanto si retira la orden como si la mantiene, el órgano jurisdiccional tendrá que informar a la autoridad emisora y al destinatario, que tendrá que ejecutarla si se mantiene. Se contempla la posibilidad de que el órgano jurisdiccional pueda pedir información a la autoridad competente del tercer Estado, siempre que ello no obstaculice el proceso penal pendiente, conforme al régimen de las transferencias de datos personales a terceros Estados u organizaciones internacionales, previsto en el Capítulo V de la Directiva (UE) 2016/680[89].

IV. LA ORDEN EUROPEA DE CONSERVACIÓN

La OEC constituye un instrumento por el que se obliga a la conservación de pruebas electrónicas, para que se pueda llevar a cabo una posterior solicitud de entrega. La autoridad emisora de un Estado miembro a través de la OEC, obliga de forma vinculante a la conservación a un proveedor que ofrezca servicios en la UE y que esté establecido o representado en otro Estado miembro (art. 2.2 PROGC)[90]. La conservación de pruebas electrónicas, consiste en impedir la retirada, supresión o alteración de datos, para poder entregarlos posteriormente a través de una OEE, una OEI[91] o de la asistencia judicial mutua (art. 6.2 PROGC), lo cual es relevante, dada la volatilidad de los datos y el riesgo de su ocultación o alteración. La OEC está estrechamente relacionada con la OEE, como se refleja, por ejemplo, en que ante determinadas incidencias que puedan surgir durante la ejecución de la OEE, se obligue a conservar las pruebas electrónicas hasta que éstas se solventen, como hemos estudiado, por

[88] *Cfr.* art. 16.5 PROGC. Se valorarán el interés específico protegido, los derechos fundamentales, la seguridad nacional, la vinculación del proceso penal donde se emitió la OEE con las jurisdicciones afectadas, nacionalidad y residencia del titular de los datos requeridos o de la víctima y el *forum delicti commisi*, entre otros.

[89] Ello constituye una acertada innovación del art. 16.5 bis PROGC (también incluida en la PRLIBE) no prevista en la PRC, que coadyuva a la coherencia de la regulación europea en materia de datos en el proceso penal.

[90] En el art. 2.2 PRLIBE, se innovan las definiciones, incorporándose las nociones de emisión o validación por la autoridad judicial y, de "Estado emisor" y "Estado de ejecución" vinculado por el Reglamento (art. 2.2)).

[91] Geraci, R. M. (2019). *Op. cit.*, pág. 1358. Existen Estados que no se han adherido a la Directiva 2014/41/UE, como Dinamarca e Irlanda, lo cual es relevante porque sobre todo Irlanda aloja a algunos de los más importantes proveedores de servicios que prestan servicios en la UE, Estado que sería fundamental en esta materia. La OEI puede ser preferible, cuando se realicen una pluralidad de actos de investigación en el Estado de ejecución, siempre que no exista riesgo de alteración de los datos. Observamos que podría emitirse la OEC para preservar los datos y que también se emita la OEI cuando conlleve la realización de un conjunto de actos de investigación.

lo que, de alguna forma, temporalmente la OEE quedaría subsumida en una OEC. Coinciden tanto la definición de autoridad emisora como la de proveedor de servicios de la OEE, entre otros aspectos, diferenciándose fundamentalmente en la finalidad, teniendo además el mismo ámbito de aplicación (art. 3 PROGC). Por tanto, la OEC versa sobre pruebas almacenadas en formato electrónico (datos de abonados, de acceso, de transacciones y de contenido), por el proveedor de servicios o en su nombre, cuando reciba el certificado de la OEC, el Anexo II (EPOC-PR)[92]. Nos centraremos básicamente en las características específicas de la OEC e iremos haciendo referencia además a aquellos aspectos comunes con la OEE que ya han sido tratados.

La determinación de la autoridad emisora no se establece en función de la categoría específica de datos sobre la que verse la OEC a diferencia de la OEE, ya que las autoridades emisoras son las mismas respecto a todas las categorías de datos, coincidiendo con las establecidas en la OEE respecto a los datos de abonado y de acceso. Por tanto, se trataría Juez, Tribunal, Juez de instrucción o Fiscal y cualquier autoridad competente definida por el Estado emisor que actúe como autoridad de investigación, estando previsto el mismo sistema de validación que hemos tratado, por un órgano jurisdiccional o Fiscal del Estado emisor (art. 4.3 PROGC), siendo el destinatario el mismo que en la OEE (art. 7 PROGC).

Existe una regulación específica de las condiciones para la emisión de la OEC, las cuales redundan igualmente en su sistema de garantías y que son más sucintas que las establecidas para la OEE. La OEC deberá responder a los principios de necesidad y proporcionalidad, pudiéndose emitir respecto a todas las infracciones penales y respecto a la ejecución de una pena o medida de seguridad privativa de libertad, con duración mínima de cuatro meses (art. 6.2 PROGC). Estas condiciones coinciden con las de la OEE referida a datos de abonados o de acceso, sin que operen las restricciones respecto a los datos de transacciones o contenido establecidas en el art. 5.4 PROGC para la OEE, lo cual repercute en la aplicación del principio de proporcionalidad en la OEC, al permitirse respecto a todas las infracciones penales[93]. Por ello, encontramos una

[92] EPOC-PR, según el acrónimo en inglés (arts. 2.6 PROGC y 2.5 PRC). En el art. 2.6) PRLIBE se las trata como "información electrónica", siendo el momento del almacenamiento el de la emisión del EPOC-PR.

[93] En el art. 6.2 PRLIBE, se establecen condiciones adicionales, entre otras, se limita a los datos de personas con vínculo directo en los procesos que entran dentro de su ámbito de aplicación. Ello constituye una forma de preservar el principio de proporcionalidad, respecto al cual se redunda en el art. 6.3 g) PRLIBE.

disfunción al respecto, dado que si bien las pruebas electrónicas respecto a los datos de transacciones y de contenido sólo podrán ser entregadas a través de la OEE si se cumplen las condiciones estudiadas, sin embargo, dichos datos sí podrán ser conservados a través de la OEC, la cual pueden emitir autoridades diferentes. La finalidad de la conservación es la posterior entrega, en la que podría repercutir esta diversidad en la regulación entre la OEE y la OEC[94]. Al margen de que ello se pueda solventar en la versión definitiva del Reglamento, con el tenor actual estimamos que, si no fuera posible entregar las pruebas electrónicas referidas a datos de transacciones o de contenido a través de la OEE, al no verificarse las condiciones del referido art. 5.4, debería acudirse a vías como la OEI o la asistencia judicial mutua, ya que no tendría mucho sentido que se permitiera la conservación y que luego no fuera posible la entrega.

La información o contenido que deberá incluir la OEC coincide sustancialmente con la de la OEE. Se trata de la autoridad emisora y/o validadora, el destinatario, el usuario, la categoría de datos que deban conservarse, el período que abarca la solicitud de conservación, las disposiciones de Derecho penal del Estado emisor y la justificación de la necesidad y proporcionalidad (art. 6.3 PROGC). Las diferencias estriban fundamentalmente, en que en la OEE se incluye además la justificación de la urgencia y el supuesto de que los datos formen parte de una infraestructura facilitada por el proveedor de servicios a una entidad distinta de una persona física. También se establece en la OEC el tratamiento previsto en la OEE para cuando los datos estén almacenados o tratados en una infraestructura que se preste a una autoridad pública, según el cual la orden sólo podrá emitirse si dicha autoridad se encuentra en el Estado emisor (art. 6.1 y 5.6 bis PROGC). No existe sin embargo, referencia alguna a los supuestos de la falta de residencia en el Estado emisor del titular de los datos solicitados ni a la protección de los datos por privilegios e inmunidades en el Estado de ejecución y las normas sobre la determinación o limitación de la responsabilidad, o que la revelación de los datos pueda afectar a la seguridad y defensa nacionales del Estado de ejecución, establecidos en la OEE, por lo que en estos supuestos los datos sí podrían ser conservados a través de la OEC[95].

[94] Fuentes Soriano, O. (2020). *Op. cit.*, págs. 318-319. Este distinto tratamiento normativo puede generar inconvenientes para la posterior entrega de los datos, planteando la conveniencia de una regulación unitaria al respecto. En un sentido similar, además, González Granda, P. (2021). *Op. cit.*, págs. 1106-1007, López Jiménez, R. (2019). *Op. cit.*, págs. 324 y 325 y Gómez Amigo, L. (2019). *Op. cit.*, págs. 38-39 y 53-54.

[95] Ello según las versiones PRC y PROGC, dado que en el art. 6.3 bis PRLIBE sí se tratan estos supuestos, respecto a los cuales se establece que no se emitirá la OEC.

En cuanto a la ejecución de la OEC, la transmisión al destinatario se efectuará a través del EPOC-PR, el cual cumplimentará la autoridad emisora o validadora, que certificará su contenido. La transmisión tendrá lugar de la misma forma que el EPOC. El EPOC-PR contendrá la información o contenido que acabamos de tratar e incluirá datos suficientes para identificar al destinatario y contactar con la autoridad emisora, sin contener justificación alguna de la necesidad o proporcionalidad ni adicionales precisiones sobre las investigaciones. En lo referente a la traducción del EPOC-PR, se establece el mismo régimen que en el EPOC (art. 8 PROGC). Tras la recepción del EPOC-PR, el destinatario deberá conservar sin demoras los datos[96] durante un plazo máximo de sesenta días, a menos que la autoridad emisora confirme que se ha iniciado una solicitud de entrega. En este caso, los datos serán conservados el tiempo necesario para su entrega[97], tras la notificación de la solicitud de la misma. La autoridad emisora tendrá que informar a la mayor brevedad, cuando la conservación ya no sea necesaria. Si surgieran incidencias que impidieran que el destinatario cumpliera su obligación, porque el EPOC-PR esté incompleto, contenga errores o no incorpore la información suficiente, el destinatario informará a la autoridad emisora a través del Anexo III, solicitando las aclaraciones necesarias, autoridad que deberá responder a la mayor brevedad en el plazo máximo de cinco días. Ello coincide con lo previsto al respecto en la OEE, al igual que el supuesto de que el destinatario no pudiera cumplir por imposibilidades derivadas de circunstancias no creadas por él o por el proveedor de servicios, en el cual igualmente se informará a la autoridad emisora a través del Anexo III, que también utilizará el destinatario para comunicar que por otros motivos diferentes

---

Estimamos que lo adecuado sería incluirlos, dado que de lo contrario se podría generar la situación de que los datos conservados luego no pudieran ser entregados.

[96] Bueno de Mata, F. (2021). *Op. cit*., pág. 40. Faltan por determinar aspectos como la tecnología para la conservación (*blockchain* y *hashgraph*) y aclarar la utilización de la OEC de forma preventiva, como forma de ciberdefensa y ciberseguridad. Estimamos que la dimensión preventiva, requiere un riguroso respeto de las garantías procesales, para evitar que la OEC se utilice de forma proactiva. También, el autor propone establecer "pautas técnicas" para el aseguramiento de la cadena de custodia electrónica en la conservación (pág. 44). González Granda, P. (2021). *Op. cit.*, págs. 1109-1110, cuestiona la falta de garantías en la cadena de custodia y que constituye uno de los aspectos más problemáticos en la prueba digital.

[97] Rogalski, M. (2020). *Op. cit*., págs. 348-349. No se incorporan salvaguardias sobre la conservación indiscriminada de los datos, no definiendo las disposiciones de forma inequívoca el período de la conservación, conforme a la jurisprudencia del TJUE (asuntos acumulados *Tele2 Sverige AB v. Post-ochtelestyrelsen*).

no conserva la información solicitada, examinando la autoridad emisora la OEC conforme a la justificación alegada (art. 10 PROGC)[98].

En la OEC posee plena aplicación el régimen de confidencialidad e información al usuario respecto al EPOC-PR y los datos conservados, en los mismos términos que en la OEE (art. 11 PROGC), el de reembolso de gastos (art. 12 PROGC) y el sistema de sanciones (art. 13 PROGC). Igualmente es aplicable el régimen del incumplimiento del EPOC-PR por el destinatario (art. 14 PROGC), siendo el mismo que el establecido en la ejecución del EPOC. La diferencia fundamental estriba en los motivos de denegación del reconocimiento o ejecución de la OEC, que se regulan de forma específica en el art. 14.5 PROGC, si bien éstos coinciden parcialmente con los de la OEE[99]. Sin embargo, no se contemplan respecto a la OEC, el procedimiento de reexamen en caso de obligaciones contradictorias (art. 16 PROGC) y las vías de recurso efectivas (art. 17 PROGC)[100]. De alguna forma, parece el legislador europeo ha prestado más atención a la OEE que a la OEC, lo cual se refleja en que el sistema de garantías en ésta sea inferior, como se comprueba en la regulación exclusiva de estas instituciones para la OEE, lo cual debería solventarse en el texto definitivo, dado que la conservación de los datos igualmente repercute en los derechos fundamentales[101]. Pensamos que la conservación de los datos podrá llegar a ser tan relevante como la propia entrega, e incluso superior, siendo en todo caso prioritario que se realice de forma correcta, lo cual permitiría la posterior admisibilidad probatoria, ya que los datos conservados podrán entregarse a través de vías diferentes a la OEE,

[98] En el art. 10 PRLIBE, se introducen novedades en la ejecución. El EPOC-PR se dirigirá al establecimiento principal o donde esté establecido el representante legal y a la autoridad de ejecución y, se prevé la prórroga de treinta días del plazo de conservación. Respecto a los defectos del EPOC-PR, si no reaccionara la autoridad emisora, la OEC se considerará nula. Si el proveedor no pueda cumplir por razones que no le sean imputables, se prevé que la autoridad emisora retire el EPOC-PR. Finalmente se contempla que el proveedor considere que el EPOC-PR no se puede ejecutar por ser manifiestamente abusivo o superar la finalidad de la orden.

[99] Consisten en que la OEC no se haya emitido o validado por la autoridad emisora, que el EPOC-PR no se pueda ejecutar por imposibilidad material o presentar errores manifiestos, que no verse sobre datos almacenados en el momento de su recepción y de que el servicio no esté cubierto por el Reglamento. Se han suprimido respecto al art. 14.5 PRC, la fuerza mayor y que el EPOC-PR fuera contrario a la CDFUE o manifiestamente abusivo.

[100] Salvo en la PRLIBE, que extiende a la OEC tanto el procedimiento de reexamen (art. 14 bis) como las vías de recurso efectivas (art. 17). Observa, González Granda, P. (2021). *Op. cit.*, pág. 1109, respecto a la PRC, que esta omisión se justifica en la mayor injerencia en los derechos de las personas afectadas que conlleva la OEE.

[101] *Cfr*. Gialuz, M. y Della Torre, J. (2018). *Op. cit.*, págs. 292 y 293.

como la OEI o la asistencia judicial, creándose una forma lógica y práctica de interacción de este nuevo instrumento con los ya existentes, que requiere una mayor atención legislativa.

V. LA DESIGNACIÓN DE LOS REPRESENTANTES LEGALES DE LOS PROVEEDORES DE SERVICIOS

Estamos ante una materia fundamental para la aplicación de la OEE y la OEC, dado que las órdenes se transmitirán por la autoridad emisora directamente a los representantes legales designados por los proveedores de servicios a efectos de recabar pruebas para procesos penales, limitándose la intervención de la autoridad del Estado de ejecución a determinadas incidencias que puedan surgir en el cumplimiento de las órdenes. No obstante, esto último no es extrapolable a la postura adoptada por la Comisión LIBE, dado que como vimos, las órdenes se transmitirán directa y simultáneamente tanto al establecimiento principal del proveedor de servicios o en su caso a su representante legal en el Estado de ejecución, como a la autoridad de ejecución (art. 7.1 PRLIBE). También tenemos que destacar que en la postura de la Comisión y del Consejo, la designación de los representantes legales se regula por una Directiva[102]. Sin embargo, como hemos tratado, en la posición adoptada por la Comisión LIBE, se rechaza la propuesta de la Comisión y se integra el contenido de la Directiva en el Reglamento, al considerarse que plantea problemas en su base jurídica, conforme a los arts. 53 y 62 TFUE. La Directiva obligaría a todos los Estados miembros a establecer representantes legales, incluyendo los que no participen en los instrumentos adoptados en aplicación del Título V, Capítulo 4 TFUE y, además dichos representantes legales no sólo tendrían virtualidad respecto al Reglamento sobre la OEE y OEC, sino que intervendrían en otros y futuros instrumentos. Ello se solventaría con dicha integración, que supondría que sólo los Estados que participen en el Reglamento, estarán obligados a designar dichos representantes[103]. A ello añadimos, como vimos, que la integración de esta

[102] Fuentes Soriano, O. (2020). *Op. cit.*, págs. 287-288. Con la designación del representante, se afronta el argumento que se suele alegar de forma dilatoria, de que el cumplimiento de la obligación solicitada afecta a la exclusividad jurisdiccional de cada Estado. La designación de los representantes legales, es importante para reducir la fragmentación existente que genera inseguridad jurídica (págs. 309-310).

[103] En la Exposición de Motivos del informe de la Comisión LIBE sobre la propuesta de Directiva, se justifica además la incorporación del contenido de la propuesta de Directiva en el Reglamento, en que constituye una "medida de acompañamiento de los instrumentos de reconocimiento mutuo", conforme al art. 82 TFUE.

materia en el Reglamento impediría que la tardía transposición por los Estados de la Directiva, pudiera afectar a la implementación práctica de las órdenes.

Vamos a tratar los representantes legales de los proveedores de servicios, considerando las distintas versiones de la propuesta legislativa, PDC, PDOGC y Comisión LIBE, en cuyo art. 6 bis PRLIBE se regulan fundamentalmente, si bien con un contenido sustancialmente más sucinto que en las otras versiones. Del mismo modo que en el estudio de las órdenes, la versión que seguiremos fundamentalmente, será la PDOGC. Ya han sido tratadas determinadas definiciones incorporadas en la propuesta de Reglamento, tales como los conceptos de "proveedor de servicios", "ofrecer servicios en la Unión" o "establecimiento o estar establecido", entre otras, que son relevantes respecto a la materia que ahora estamos tratando, dado que es necesario que dichos proveedores posean un vínculo suficiente con la UE, a las que nos remitimos, ya que reproducen *mutatis mutandis* las definiciones del art. 2 PDOGC y PDC.

La propuesta de Directiva establece las normas armonizadas relativas a la designación de representantes legales de los proveedores de servicios[104] para la recepción, cumplimiento y ejecución de las resoluciones y órdenes emitidas por las autoridades de los Estados miembros, a efectos de recabar pruebas para los procesos penales. Dicha Directiva se aplicará a los proveedores de servicios que los ofrezcan en la UE, no aplicándose cuando éstos únicamente estén establecidos en el territorio de un único Estado miembro y exclusivamente presten sus servicios en él, sin perjuicio de que conforme al Derecho nacional y el Derecho de la UE las autoridades emisoras se puedan dirigir directamente a los proveedores de servicios establecidos en su territorio, es decir, sin seguir el cauce de la representación legal (art. 1 PDOGC). La figura del "representante legal", sería la "persona jurídica o física designada por escrito por un proveedor de servicios", a los referidos efectos de dichas órdenes (art. 2.1 PDOGC). Los Estados miembros en los que esté establecido un proveedor que preste servicios en la UE, tendrán que garantizar que dicho proveedor designe al menos un representante legal, el cual tendrá que residir o estar establecido en uno de los Estados miembros en los que el proveedor esté establecido u ofrezca sus servicios (art. 3.1 PDOGC). Es decir, no

[104] López Jiménez, R. (2019). *Op. cit.*, págs. 330-331. La designación del representante legal, conlleva un eficaz mecanismo para permitir que las órdenes se notifiquen, siendo necesaria al no existir el requisito legal de que los proveedores de terceros países estén presentes físicamente en la UE para la prestación de servicios. También, entre otros, Gialuz, M. y Della Torre, J. (2018). *Op. cit.*, págs. 290 y 291.

es necesario que dicho representante se establezca en cada uno de los Estados donde se ofrezcan dichos servicios, sino en uno de ellos. Ello consideramos que podría plantear problemas operativos, dado que es posible que el proveedor ofrezca sus servicios en varios Estados, por lo que quizá sería recomendable que en cada Estado miembro donde se presten dichos servicios, exista al menos un representante designado. Ya vimos los requisitos de la OEE y OEC, tales como la lengua en la que se emitirán o las intervenciones previstas de la autoridad de ejecución, a lo cual se suma el previsible importante volumen de número de órdenes que se emitan. Por ello, creemos que para facilitar la ejecución de dichas órdenes y respetar sus estrechos plazos, podría ser recomendable que exista un representante por cada Estado miembro si en él se prestan los referidos servicios. La designación de representantes legales adicionales cuando se ofrezcan servicios o los prestadores de servicios estén establecidos en otros Estados miembros, se contempla como algo opcional, existiendo también la posibilidad de que los proveedores de servicios designen de forma colectiva un representante legal (art. 3.4 PDOGC)[105].

En el supuesto de que el proveedor de servicios no esté establecido en la UE pero ofrezca servicios en el territorio de sus Estados miembros, dichos Estados tendrán que asegurar que el proveedor designe al menos un representante legal en la UE, que del mismo modo residirá o tendrá que establecerse en uno de los Estados miembros donde se presten los servicios (art. 3.2 PDOGC)[106]. Como hemos estudiado, los representantes legales se designan a los efectos de la recepción, cumplimiento y ejecución de las resoluciones y órdenes emitidas en el marco de los instrumentos jurídicos que estén dentro del ámbito de aplicación del Capítulo 4, Título V TFUE, a los efectos de recabar pruebas en los procesos penales (art. 3.3 PDOGC), lo cual, como vimos, constituye un extremo cuestionado en la postura de la Comisión LIBE[107]. En la PDOGC se establecen numerosas obligaciones para los Estados miembros respecto a los proveedores de servicios y sus representantes legales, que velarán porque las resoluciones y órdenes se dirijan al representante legal designado, al cual se le confiará tanto la recepción, como su cumplimiento en nombre del

[105] La designación colectiva de un representante legal, se reserva para los proveedores de servicios que formen parte de un Grupo, en los arts. 3.4 PDC y 6 bis.3 PRLIBE.

[106] En un sentido similar, art. 6 bis.1 PRLIBE. Si el proveedor está establecido en un Estado no vinculado por el Reglamento, el representante legal se establecerá en uno de los Estados vinculados (art. 6 bis.2 PRLIBE).

[107] En el art. 6 bis PRLIBE, las funciones del representante legal se limitan exclusivamente a la recepción, cumplimiento y ejecución de la OEE y OEC, en nombre del proveedor de servicios.

proveedor de servicios, pudiendo ser objeto de medidas de ejecución (art. 3.5 PDOGC). Para ello los Estados donde residan o estén establecidos los proveedores de servicios, garantizarán que éstos doten al representante legal de las competencias y recursos necesarios, que cooperen con las autoridades competentes (art. 3.6 y .7 PDOGC) y, que tanto el representante legal como el proveedor de servicios, puedan ser responsables solidarios por el incumplimiento de las obligaciones establecidas cuando reciban las decisiones y órdenes. Esta responsabilidad no se limita a la OEE y OEC, abarcando otros instrumentos como la OEI[108], los cuales podrán ser sancionados, salvo que incurrieran en responsabilidad penal, supuesto en el que no se aplicará el régimen de responsabilidad solidaria (art. 3.8 PDOGC). Los Estados miembros garantizarán que la designación de los representantes legales tenga lugar en el plazo de seis meses desde la fecha de transposición de la Directiva, salvo que los proveedores comiencen a ofrecer sus servicios en la UE tras dicha fecha (art. 3.9 PDOGC)[109].

Una vez designado el representante legal, el proveedor establecido o que ofrezca sus servicios en un Estado, notificará a la autoridad central del Estado miembro en el que resida o esté establecido el representante legal, tanto la designación como los datos de contacto del representante y la lengua o lenguas oficiales de la UE en las que puede dirigirse a él, incluyéndose una o más lenguas oficiales conforme a la legislación nacional de dicho Estado miembro (art. 4.1 y 4.2 PDOGC)[110]. De forma análoga, en el caso de que el proveedor de servicios designara varios representantes legales, en la notificación se deberá indicar la lengua o lenguas oficiales de la UE, de los Estados miembros asignados a cada representante legal y a qué representante haya que dirigirse, si bien las autoridades competentes podrán "apartarse" de dichas consideraciones en casos específicos, en los cuales los Estados tendrán que velar por el cumplimento de lo que

[108] Sobre la extensión de este sistema de responsabilidad, Bueno de Mata, F. (2021). *Op. cit.*, pág. 42.

[109] Este plazo constituye una novedad de la PDOGC, donde se incorporan innovaciones respecto al art. 3 PDC, como la referencia a las medidas de ejecución del art. 3.5, la nueva redacción de los apartados 6 y 7 y el sistema de responsabilidad solidaria. En el art. 6 bis PRLIBE no se efectúa referencia alguna a ello.

[110] Los Estados miembros velarán por el cumplimiento de estas obligaciones. La determinación de la lengua se efectuará conforme al Reglamento 1/58. Si bien ello concuerda con lo establecido respecto a la traducción del EPOC o del EPOC-PR, en el art. 8.5 PROGC, se contempla la posibilidad de que no se haya especificado ninguna lengua por el destinatario y en el art. 18 bis se prevé que la transmisión del EPOC, EPOC-PR, OEE u OEC, se efectúe en un idioma distinto de la lengua o lenguas oficiales del Estado miembro. Encontramos un diferente tratamiento respecto al tenor del art. 4.2 PDOGC, que estimamos debería solventarse.

se requiera al representante legal (art. 4.3 PDOGC). Toda esta información tiene que estar disponible y actualizada en una página específica de la web de la Red Judicial Europea[111], por lo cual tendrán que velar los Estados miembros (art. 4.4 PDOGC).

Respecto al incumplimiento de las obligaciones por los proveedores de servicios y sus representantes legales, los Estados miembros tendrán que crear un sistema de sanciones que serán efectivas, proporcionadas y disuasorias, adoptando las medidas para garantizar su ejecución, el cual tendrán que comunicar a la Comisión Europea (art. 5 PDOGC). Además, para garantizar que la Directiva se aplique de forma coherente y proporcionada, los Estados miembros designarán una o varias autoridades centrales[112] comunicándolo a la Comisión, la cual enviará a los Estados la lista de dichas autoridades, publicándola con la finalidad de facilitar las notificaciones expuestas por los proveedores de servicios a los Estados miembros. Las autoridades centrales de los Estados miembros, deberán coordinarse y cooperar tanto entre ellas como con la Comisión, facilitándose la información y asistencia necesaria, incluyéndose las medidas de ejecución (art. 6 PDOGC).

VI. CONCLUSIONES

En el desarrollo de este trabajo hemos estudiado con detalle las características e innovaciones fundamentales que supone este nuevo instrumento para la obtención transnacional de la prueba electrónica en la UE, abordando los distintos aspectos en los que incide y efectuando las oportunas consideraciones y conclusiones. Resaltamos que la creación de este instrumento, inaugura un nuevo modelo donde la cooperación directa con los proveedores de servicios, constituye una importante innovación. Pero ello no está exento de riesgos, por lo que desde una perspectiva procesal como propuestas de mejora de la normativa, estimamos que debe-

[111] Dichas notificaciones sobre los datos del representante legal, la lengua oficial y la publicación en una página específica, se establecen igualmente, en los apartados 5 a 7 del art. 6 bis PRLIBE.

[112] El sistema sancionador de los Estados, aunque está en consonancia con el previsto para el incumplimiento del EPOC y EPOC-PR en el art. 13 PROGC, a diferencia de éste no especifica que las sanciones serán de carácter pecuniario ni su límite *ad quem*, por lo que consideramos que deberían armonizarse las previsiones de la PDOGC y de la PROGC. En el art. 6 bis.8 y .9 PRLIBE, la regulación es diferente y más sucinta, estableciéndose que los Estados establecerán un sistema sancionador similar al indicado y garantizarán que el representante legal pueda ser considerado responsable, al margen de la responsabilidad del proveedor de servicios.

rían implementarse las necesarias cautelas para preservar el sistema de garantías procesales del acervo normativo de la UE, instaurándose eficaces mecanismos procesales que profundicen en el sistema de protección de datos en los procesos penales y respondan a los principios de necesidad, proporcionalidad y especialidad, al derecho de defensa, la tutela judicial efectiva y los derechos fundamentales consagrados en la CDFUE. Ello tendría beneficios relevantes para la posterior admisibilidad probatoria y, por tanto, en la propia efectividad de este instrumento. Por ello consideramos que sería también muy beneficioso que el legislador europeo solventara la actual fragmentación de la normativa procesal en materia de obtención y admisión de la prueba en los Estados miembros, aproximando las regulaciones procesales internas. Pero además es necesario que se mejore la regulación procesal de la conservación de los datos, de la cadena de custodia digital, que se establezcan límites temporales precisos sobre los períodos de conservación, que se creen sólidos canales de comunicación para la entrega de pruebas electrónicas y que se instaure un eficaz sistema de recursos tanto en el Estado de emisión como en el de ejecución, que tutele los derechos de los titulares de los datos, que supere de forma sustancial al inicialmente previsto.

Proponemos, además, que se profundice en la aplicación procesal del principio de proporcionalidad, para impedir la utilización de la OEE y OEC en delitos de escasa gravedad. En este sentido, consideramos que deberían armonizarse los requisitos procesales para la emisión de la OEE y la OEC, de tal forma que el sistema de garantías fuera equivalente en ambas, respecto a todas las categorías de datos, dado que éste es más elevado en la OEE, lo cual evitaría la conservación indiscriminada de datos y las posteriores dificultades procesales para la entrega. Dicho principio debería ostentar un lugar esencial como el eje vertebrador de todo el sistema, constituyendo además una forma de conciliar la seguridad, la cual ostenta una posición preeminente en el ELSJ y, que parece prioritaria en este nuevo instrumento, con la libertad y la justicia. Por ello creemos necesario además que se redefinan las categorías de datos, para evitar imprecisiones o interpretaciones procesales ambiguas en la práctica. Ello fomentaría la confianza mutua entre los Estados, la cual se requiere en un alto grado en este instrumento.

La peculiar reinterpretación del principio de reconocimiento mutuo que se incorpora en las versiones iniciales de la propuesta de Reglamento, con la ejecución directa de las órdenes por los representantes legales de los proveedores de servicios, nos hace plantearnos si realmente estamos ante un instrumento de esta índole. Por ello creemos que su concepción

podría mejorar sustancialmente, implementándose la intervención de las autoridades judiciales del Estado de ejecución en todos los supuestos, lo cual constituiría una eficaz solución procesal a la problemática que supone encomendar a los proveedores de servicios la verificación de los requisitos procesales de las órdenes, que redundaría en el sistema de garantías, debiendo mejorarse para ello el sistema de notificaciones. Además, proponemos recuperar la clásica lista de treinta y dos delitos en los que no se efectuará el control de la doble tipificación, e incluso implementar motivos de denegación del reconocimiento y ejecución análogos a los de otros instrumentos como la OEI, todo lo cual permitiría procesalmente incardinar fácilmente este nuevo instrumento en la Ley 23/2014, de reconocimiento mutuo de resoluciones penales.

Queda por ver, no obstante, cuál será la naturaleza, concepción y diseño de este nuevo instrumento, cuando el legislador europeo promulgue la versión definitiva del Reglamento, dado que parte de estas cuestiones se solventarían en la versión de la Comisión LIBE del Parlamento Europeo. De cualquier forma, la nueva figura del representante legal de los proveedores de servicios constituye una institución fundamental e incuestionada por el legislador europeo, que ostentará una función primordial en el cumplimiento de las órdenes y que solventa los inconvenientes prácticos actuales que las autoridades enfrentan para obtener la prueba electrónica a través de los cauces procesales vigentes. Pero creemos que quedan por mejorar aspectos tales, como los mecanismos para las solicitudes de reembolso de gastos, que es necesario implementar reglas que armonicen los futuros sistemas sancionadores de los Estados respecto al incumplimiento de las órdenes por los proveedores y, que la designación de representantes de los mismos en cada Estado donde presten servicios no sea algo opcional, sino obligatorio, lo cual facilitaría enormemente la dimensión procesal de la ejecución de las órdenes. Otra cuestión fundamental estriba en limitar la intervención de dichos representes legales únicamente a estas órdenes, o bien extenderla a todos los instrumentos actuales e incluso futuros, del mismo modo que la técnica legislativa seguida para crear esta figura: una Directiva, según la postura de la Comisión Europea y del Consejo de la Unión Europea o bien, incorporarla en el Reglamento, como defiende la Comisión LIBE, solución que consideramos más adecuada.

Consideramos que las futuras OEE y OEC, que responden a una problemática y a retos de gran envergadura, ostentarán previsiblemente un papel esencial en el ELSJ, de ahí la gran importancia del respeto de las garantías procesales del mismo modo que de principios como el de pro-

porcionalidad, para poner en valor la libertad y justicia en un entorno que parece dominado por la seguridad, pudiendo servir además como útil herramienta para al menos aproximar las garantías procesales en el ámbito de la admisibilidad probatoria en los Estados miembros, lo cual arrojaría beneficios nada despreciables en el ELSJ. Ello constituye igualmente un reto para el legislador europeo, que tendría efectos muy positivos para la lucha contra las distintas formas de ciberdelincuencia y el terrorismo internacional y, que también forma parte obviamente de la problemática procesal de la obtención transnacional de la prueba electrónica, respecto a la cual hemos efectuado las referidas propuestas de mejora.