Revista de Estudios Europeos
Publicación del Instituto Universitario de Estudios Europeos de la Universidad de Valladolid
EDICIONES Universidad Valladolid

Las órdenes europeas de producción y de conservación de prueba electrónica transfronteriza en los procesos penales en la Unión Europea*

The European Production and Preservation Orders of cross-border electronic evidence in criminal proceedings in the European Union

ÁNGEL TINOCO PASTRANA
Profesor Titular de Derecho procesal. Universidad de Sevilla
atinoco@us.es
ORCID: 0000-0002-6622-9030
Recibido: 20/04/2025. Aceptado: 11/06/2025.
Cómo citar: Tinoco Pastrana, Ángel, "Las órdenes europeas de producción y de conservación de prueba electrónica transfronteriza en los procesos penales en la Unión Europea", *Revista de Estudios Europeos* 86 (2025): 130-158.
Este artículo está sujeto a una licencia "Creative Commons Reconocimiento-No Comercial" (CC-BY-NC).
DOI: https://doi.org/10.24197/ree.86.2025.130-158

Resumen: Las órdenes europeas de producción y de conservación de prueba electrónica transfronteriza en los procesos penales, inauguran un nuevo modelo de cooperación directa público-privada entre las autoridades judiciales del Estado de emisión y los prestadores de servicios de comunicaciones electrónicas y de la sociedad de la información en la Unión Europea, que requiere un alto grado de confianza mutua entre los Estados miembros. Las nuevas órdenes responden a la necesidad acuciante existente en el Espacio Europeo de Libertad, Seguridad y Justicia, de crear un ágil y simplificado sistema para la obtención y conservación transfronteriza de la prueba electrónica. El *"e-evidence package"*, resultado de un lento y complejo procedimiento legislativo, posee una importante repercusión en los prestadores de servicios, que tendrán que designar establecimientos y representantes legales para la recepción y ejecución de las órdenes. Éstos adquieren un gran protagonismo en el nuevo modelo de cooperación creado.
Palabras clave: prueba electrónica; orden europea de producción; orden europea de conservación; prestadores de servicios; confianza mutua.

* Este trabajo se ha realizado en el marco del Proyecto de Investigación "El Derecho Procesal Civil y Penal desde la perspectiva de la Unión Europea: la consolidación del Espacio de Libertad, Seguridad y Justicia (CAJI)", Proyecto I+D+i PID2021-124027NB-I00, Agencia Estatal de Investigación, Ministerio de Ciencia e Innovación.

Abstract: European Production and Preservation Orders for cross-border electronic evidence in criminal proceedings introduce a new model of direct public–private cooperation between the judicial authorities of the issuing state and providers of electronic communications and information society services within the European Union. This model requires a high degree of mutual trust between Member States. These new orders address the urgent need within the European Area of Freedom, Security and Justice for a streamlined, simplified system for gathering and preserving electronic evidence across borders. The 'e-evidence package', the product of a lengthy and complex legislative process, will have a significant impact on service providers, who will be required to appoint establishments and legal representatives to receive and execute orders. These entities will play a pivotal role in the new cooperation model.

Keywords: electronic evidence; European Production Order; European Preservation Order; service providers; mutual trust.

INTRODUCCIÓN

Las nuevas órdenes europeas de producción y de conservación (OEP, OEC), constituyen innovadores instrumentos concebidos para la obtención y conservación de la prueba electrónica transfronteriza de naturaleza penal en la Unión Europea (UE), creados por el Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023[1] (Reglamento e-evidence), cuya aplicación tendrá lugar a partir del 18 de agosto de 2026. De forma preliminar, observamos que las órdenes inauguran un nuevo modelo de cooperación directa público-privada entre las autoridades judiciales del Estado emisor y los prestadores de servicios de comunicaciones electrónicas y los prestadores de servicios de la sociedad de la información que los ofrezcan en la UE. Este modelo no respondería a la tradicional concepción y diseño de los instrumentos de reconocimiento mutuo, limitándose la intervención de la autoridad judicial del Estado de ejecución a determinados supuestos específicos en los que será notificada (arts. 7 y 8 Reglamento e-evidence), lo cual sería incluso de carácter marginal, modelo que posee relevantes simetrías con la *US Cloud Act* de 2018. De ahí la importancia de establecer normas armonizadas para la designación de establecimientos y de representantes legales de los prestadores de servicios, los cuales son fundamentales para el

[1] Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. DOUE de 28 de julio de 2023, L 191, pp. 118-180, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

funcionamiento de las nuevas órdenes, materia que se regula por la coetánea Directiva (UE) 2023/1544, del Parlamento Europeo y del Consejo, de 12 de julio de 2023[2]. La Directiva tendrá que estar transpuesta en los ordenamientos de los Estados Miembros dentro de la fecha límite del 18 de febrero de 2026, por tanto, de forma previa a la aplicación del Reglamento e-evidence.

Ello supone una importante tarea para los Estados, con los conocidos riesgos derivados de la tardía transposición de las Directivas, del mismo modo que para los prestadores de servicios, empresas privadas en suma, que tendrán que efectuar importantes actuaciones en un reducido espacio temporal, dada la proximidad de la fecha para la aplicación tanto de la Directiva como del Reglamento. Ésta no ha sido concebida únicamente para la aplicación del Reglamento e-evidence, ya que su eficacia se extiende a la prueba electrónica que se obtenga a través de la Directiva 2014/41/UE, relativa a la orden europea de investigación (DOEI)[3], del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la UE[4], del mismo modo que a las resoluciones y órdenes para recabar pruebas electrónicas en procesos estrictamente nacionales[5].

[2] Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales. DOUE de 28 de julio de 2023, L 191, pp. 181-190, ELI: http://data.europa.eu/eli/dir/2023/1544/oj.

[3] DOUE de 1 de mayo de 2014, L 130, pp. 1-36, ELI: http://data.europa.eu/eli/dir/2014/41/oj.

[4] Convenio celebrado por el Consejo de conformidad con el artículo 34 del Tratado de la Unión Europea. DOCE de 12 de julio de 2000, C 197, pp. 3-23.

[5] La extensión del ámbito de aplicación de la Directiva (art. 1.2), estimamos que constituye un importante progreso en aras de facilitar la obtención de la prueba electrónica en materia penal, con independencia del instrumento utilizado o del ámbito nacional o transfronterizo del proceso penal específico. Ello favorecerá la labor tanto de las autoridades judiciales como de los prestadores de servicios de comunicaciones electrónicas y los prestadores de servicios de la sociedad de la información, al crearse un sistema homogéneo de interlocución en la materia, que contribuye a la mejora de la obtención de la fuente de prueba electrónica almacenada. Ésta constituye una fuente de prueba que desde hace años ha adquirido gran protagonismo en las investigaciones penales y que requiere de mecanismos rápidos y eficaces, dada su volatilidad, facilidad de ocultación y destrucción entre otros factores, mecanismos que requieren que se mejore la colaboración de los prestadores de servicios con las autoridades judiciales. Como veremos, las nuevas OEP y OEC coexistirán tanto con la orden europea de investigación como con la asistencia judicial, creándose una lógica interacción y complementariedad entre los diversos mecanismos para la obtención transfronteriza de la prueba electrónica.

Estos instrumentos legislativos constituyen el fruto de un arduo procedimiento legislativo de cinco años de duración, que se remonta a las propuestas de Reglamento y Directiva de la Comisión Europea de abril de 2018[6], cuyo germen estriba en la lucha contra el terrorismo internacional, en concreto 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, realizada dos días después de los atentados terroristas de Bruselas[7]. Pero como vemos tendremos que esperar más de diez años desde dicha fecha para la efectividad real de las nuevas órdenes. En el lento procedimiento legislativo existieron profundas discrepancias entre los colegisladores europeos, Consejo de la Unión Europea y Parlamento Europeo (Comisión LIBE)[8], sobre la naturaleza y concepción de las OEP y OEC. Entre otros aspectos, el debate se centró en el papel de las autoridades judiciales del Estado de ejecución, dado el referido modelo de cooperación directa público-privada que se instaura, en la propia concepción y diseño de estos nuevos instrumentos que como tales están alejados de los tradicionales instrumentos de reconocimiento mutuo, en la incorporación de la tradicional lista de treinta y dos delitos en los que no se efectúa el control de la doble tipificación, la cual si bien ha sido incluida en el Reglamento e-evidence, no se contemplaba ni en la propuesta de Reglamento de la Comisión ni en la Orientación General del Consejo sobre la misma, además en el propio sistema de garantías en cuanto al acceso y

[6] 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, Estrasburgo, 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, Estrasburgo, 17 de abril de 2018, 2018/0107 (COD). Se trata del "*e-evidence package*" presentado por la Comisión para la obtención de la prueba electrónica, propuestas legislativas efectuadas tras la petición formulada en las conclusiones del Consejo de la Unión Europea de 20 de noviembre de 2017 (doc. nº 14435/17).

[7] *Vid* https://www.consilium.europa.eu/es/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/ (fecha de consulta: 15/04/2025).

[8] Hasta el 25 de enero de 2023, no se llegó a un Acuerdo entre el Consejo y el Parlamento sobre las propuestas de Reglamento y Directiva. Vid. https://www.consilium.europa.eu/en/press/press-releases/ (fecha de consulta: 15/04/2025).

transmisión de los datos conforme al principio de proporcionalidad[9]. La referida compleja tramitación legislativa ha acrecentado la necesidad apremiante existente desde hace lustros, de crear un moderno y eficiente sistema para la obtención transfronteriza de la prueba electrónica de naturaleza penal en la UE, ámbito en el cual son claramente insuficientes los instrumentos y mecanismos existentes, tales como la orden europea de investigación (OEI).

Son numerosas las novedades y las cuestiones relativas a la repercusión de las nuevas órdenes en la concepción y evolución del modelo de la cooperación judicial en la UE, además del propio mecanismo de emisión y ejecución de las OEP y OEC, que requieren atención y serán estudiadas en este trabajo.

1. EL SISTEMA DE TRANSMISIÓN DIRECTA DE LAS ÓRDENES POR LAS AUTORIDADES DE EMISIÓN A LOS ESTABLECIMIENTOS Y REPRESENTANTES LEGALES DE LOS PRESTADORES DE SERVICIOS

Las OEP y OEC conllevan una gran simplificación del procedimiento respecto a los instrumentos previamente existentes. Éstas permiten que la autoridad del Estado de emisión ordene directamente la entrega o conservación de las pruebas electrónicas al establecimiento designado o al representante legal del prestador de servicios que los ofrezca en la UE, con independencia de donde se ubiquen los datos (*cfr. et al.* arts. 1 y 7.1 Reglamento e-evidence), lo cual es especialmente relevante dada su deslocalización, almacenamiento en la nube y volatilidad, entre otros factores. La prueba electrónica se define como los "datos de abonados, datos de tráfico y datos de contenido", almacenados por el prestador de servicios o en su nombre, en el momento de recibir los certificados de la orden europea de producción (EPOC) o de la orden europea de conservación (EPOC-PR) (art. 3.8) Reglamento e-evidence). A los datos de abonados se equiparan los datos solicitados con el único fin de identificar al usuario (art. 3.10) Reglamento e-evidence).

La designación de establecimientos y de representantes legales de los prestadores de servicios de comunicaciones electrónicas y los

[9] *Vid.* Forlani, Gianluca (2023). "The E-evidence Package. The Happy Ending of a Long Negotiation Saga". EUCRIM. 2, 174-181. Sippel, Birgit (2023). "Guest Editorial". EUCRIM. 2, 109.

prestadores de servicios de la sociedad de la información que los ofrezcan en la UE, para la recepción y ejecución de las resoluciones y órdenes emitidas por las autoridades de los Estados miembros, constituye una eficaz solución para la notificación de las órdenes sin que ello suponga una excesiva carga para los prestadores, facilitando la libre prestación de servicios además de resolver la fragmentación jurídica actual en la materia[10]. La Directiva (UE) 2023/1544, se aplicará a los prestadores 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 el mismo[11]. El establecimiento designado constituye un establecimiento con personalidad jurídica designado por escrito por un prestador de servicios que esté establecido en un Estado miembro. La figura del representante legal sería la persona jurídica o física designada por escrito por un prestador de servicios cuando el mismo no esté establecido en el Estado miembro que participa en Reglamento e-evidence, DOEI o en el Convenio relativo a la asistencia judicial mutua en materia penal[12]. Se establecen numerosas obligaciones de los Estados miembros respecto a los prestadores de servicios, que tendrán que velar porque éstos designen a los establecimientos y representantes legales, además de crear un sistema sancionador y designar a las autoridades centrales[13].

[10] *Vid.* considerando nº 2 de la Directiva (UE) 2023/1544.

[11] *Cfr.* art. 1.5 de la Directiva (UE) 2023/1544.

[12] *Vid.* art. 3.6 y .7 del Reglamento e-evidence y art. 2.5 y .6 de la Directiva (UE) 2023/1544. Cabe la posibilidad de que el prestador de servicios no esté establecido con personalidad jurídica en la UE, pero que ofrezca servicios en el territorio de sus Estados miembros, supuesto en el que dichos Estados tendrán que asegurar que dicho prestador designe uno o varios representantes legales (art. 3.1,b) Directiva (UE) 2023/1544).

[13] Los Estados velarán entre otras cuestiones, porque las resoluciones y órdenes se dirijan al establecimiento designado o al representante legal y que la designación de los establecimientos y representantes legales de los prestadores de servicios que los ofrezcan en la UE a 18 de febrero, tenga lugar a más tardar el 18 de agosto de 2026, salvo que los prestadores hayan comenzado a ofrecer sus servicios en la UE tras dicha fecha, supuesto en el que tendrán seis meses para efectuar dicha designación (art. 3.2 Directiva (UE) 2023/1544). Respecto al incumplimiento de las obligaciones por los prestadores de servicios y sus representantes legales, los Estados miembros tendrán que crear un sistema de sanciones que serán efectivas, proporcionadas y disuasorias (art. 5 Directiva (UE) 2023/1544), sistema que comunicarán a la Comisión a más tardar el 18 de febrero de 2026. Para garantizar que la Directiva se aplique de forma coherente y proporcionada, los

El reconocimiento y ejecución por parte de la autoridad judicial del Estado de ejecución no es necesario en las OEP y OEC, el cual se sustituye por la transmisión directa a los representantes y establecimientos de los prestadores de servicios, junto con la simultánea notificación a la autoridad de ejecución únicamente si la OEP versa sobre datos de tráfico y de contenido (art. 8 Reglamento e-evidence). Ésta verificará si concurre alguno de los motivos de denegación específicos, aunque incluso en éstos existen importantes matices y excepciones que finalmente conllevan que dicho control por la autoridad judicial de ejecución sea en gran medida de carácter residual, sin desvirtuarse realmente el modelo de cooperación directa público-privado creado. Los plazos para la entrega de los datos solicitados a través de la OEP se establecen en diez días con carácter general y en ocho horas para supuestos urgentes desde la recepción del EPOC (art. 10.2 y .4 Reglamento e-evidence). La conservación de los datos será inmediata tras la recepción del EPOC-PR (art. 11.1 Reglamento e-evidence). Ello contrasta con los ciento veinte días que conlleva la OEI y los diez meses de la asistencia judicial[14].

Este sistema en parte, poseería una dinámica con analogías respecto a la OEI referida a la intervención de las telecomunicaciones sin la asistencia técnica del "Estado notificado", en el cual la autoridad judicial del "Estado que realiza la intervención", la efectúa de forma directa sin que exista un sistema de reconocimiento y ejecución por parte la autoridad competente del Estado notificado[15]. No obstante, en este caso se trata de obtención de pruebas en tiempo real, lo cual no se permite a través de las OEP y OEC, dado que éstas únicamente permiten la obtención de datos almacenados por el prestador de servicios cuando reciba el certificado de

Estados miembros designarán una o varias autoridades centrales comunicándolo a la Comisión (art. 6 Directiva (UE) 2023/1544).

[14] *Vid. Factsheet e-evidence*: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345 (fecha de consulta: 15/04/2025).

[15] *Cfr.* arts. 31 DOEI, 204 y 222 Ley 23/2014, de reconocimiento mutuo. La autoridad que realiza la intervención, podrá notificar que la persona cuyas comunicaciones se intervienen, se encuentra o encontrará en su territorio. En esta intervención de telecomunicaciones observamos que no estaríamos ante una OEI en sentido estricto al flexibilizarse sus requisitos, dado que los plazos de reconocimiento y ejecución aquí no tienen sentido, aunque sí entraría dentro del ámbito de aplicación de la Directiva.

la orden, impidiéndose la retención generalizada e indiscriminada de datos del mismo modo que la interceptación u obtención de datos tras la recepción de las órdenes[16], en consecuencia, las investigaciones prospectivas o "*fishing expedition*".

Consideramos que el mecanismo procedimental de los tradicionales instrumentos de reconocimiento mutuo sería inadecuado para la obtención y conservación de datos electrónicos, dada su volatilidad y facilidad de ocultación y destrucción, entre otros factores, el cual si bien pensamos que sería adecuado para la detención y entrega de personas a través de la orden europea de detención y entrega, no sería eficaz para la obtención transfronteriza de la prueba, máxime si se trata de prueba electrónica. Las OEP y OEC estimamos que conllevan un replanteamiento del principio de reconocimiento mutuo que incluso nos puede llevar a concluir que realmente no estaríamos *stricto sensu* ante un instrumento de esta índole, fundamentalmente cuando se trata de conservar los datos y de obtener datos de abonados y de datos almacenados con el único fin de identificar al abonado, ya que en estos supuestos no se notificará el certificado de la orden a la autoridad del Estado de ejecución, sino ante un instrumento de naturaleza diversa fundamentado en la confianza mutua entre los Estados. En este sentido, es significativo que en el Reglamento e-evidence se identifique como el mecanismo que permite la remisión directa de las órdenes por las autoridades a los prestadores de servicios, al "principio de confianza mutua" entre los Estados miembros junto con la "presunción del respeto" por los Estados del Derecho de la UE, del Estado de Derecho y de los derechos fundamentales[17]. Por ello estimamos que las nuevas órdenes podrían definirse como un nuevo tipo de instrumento de cooperación judicial o un nuevo subtipo de instrumento de reconocimiento mutuo, que requiere un alto nivel de confianza mutua entre los Estados[18] en el Espacio de Libertad, Seguridad y Justicia (ELSJ). No obstante con independencia de la definición de la naturaleza de las OEP y OEC, éstas ciertamente conllevan un "cambio de modelo" en la cooperación

[16] *Vid.* considerando nº 19 del Reglamento e-evidence.
[17] *Cfr*. considerando nº 12 del Reglamento e-evidence.
[18] Al respecto, *vid.* Tinoco Pastrana, Ángel. (2021). "Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea". *Cuadernos de Política Criminal*. 135, 210.

transfronteriza en la UE[19], dada la sustitución del modelo de cooperación entre autoridades judiciales por el nuevo sistema de cooperación público-privado de éstas con los prestadores de servicios.

Precisamente ésta constituyó una cuestión controvertida durante la tramitación legislativa del *e-evidence package*, con numerosas opiniones críticas sobre el cambio de paradigma que conlleva este nuevo modelo de cooperación[20]. Del mismo modo la Comisión LIBE del Parlamento Europeo formuló relevantes enmiendas respecto a la propuesta de Reglamento, en cuyo informe en gran medida, se concebía a las futuras órdenes europeas con un diseño y concepción más próximo al de los tradicionales instrumentos de reconocimiento mutuo. Por ejemplo, se incorporaba la remisión directa y simultánea en todos los supuestos tanto al prestador de servicios como a la autoridad de ejecución, además de otras múltiples cuestiones, como la recuperación de la tradicional lista de los treinta y dos "eurodelitos" incluida en los instrumentos de reconocimiento mutuo en los que no se efectuará el control de la doble tipificación, la cual

[19] En este sentido, De Hoyos Sancho, Montserrat. (2024). *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Analisis y valoración del "e-evidence package"*. Las Rozas. Aranzadi. 23-24.

[20] *Vid.* entre otros, Daniele, Marcelo (2019). "L´acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale". *Revista Brasileira de Direito Processual Penal*. 5 (3), 1282-1283; Geraci, Rosa Maria (2019). "La circulazione transfrontaliera delle prove digitali in UE: La proposta di Regolamento e-evidence". *Cassazione penale*, 59 (3), 1349-1350; Mitsilegas, Valsamis (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*, 25 (3), 264; Tosza, Stanislaw (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*, 11 (2), 178, 181; Stefan, Marco y Gloria González Fuster (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*, November (updated in May 2019), Bruselas, Centre for European Policy Studies. 30-32; De Hoyos Sancho, Montserrat (2022). "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal". *Revista General de Derecho procesal*. 58, 23-25; Fuentes Soriano, Olga (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*, Valencia, Tirant lo Blanch. 307.

no se contemplada en la propuesta de Reglamento e-evidence[21]. Como resultado de ello, en el Reglamento e-evidence se incorporó la notificación obligatoria del EPOC a la autoridad de ejecución cuando verse sobre datos de tráfico y de contenido, del mismo modo que se recuperó la referida lista de treinta y dos eurodelitos, entre otras innovaciones respecto a la propuesta inicial.

Nos planteamos si el diseño y la concepción definitiva de las OEP y OEC es la adecuada para los fines para los que han sido concebidas, dado que ello constituye el resultado final de la compleja tramitación legislativa y las discrepancias entre los colegisladores europeos. En la versión inicial observamos que en gran medida se intentó reproducir el modelo de la *US Cloud Act* de 2018 "Ley de clarificación del uso legítimo de los datos fuera de los Estados Unidos". Estados Unidos es quien recibe el mayor número de solicitudes de prueba electrónica de la UE y conforme a la legislación estadounidense, actualmente los prestadores de servicios únicamente proporcionan de forma voluntaria datos sin contenido[22]. Por ello nos resulta especialmente interesante, la vinculación de esta materia con el mandato otorgado por el Consejo de la UE a la Comisión en junio de 2019, para negociar un Acuerdo entre la UE y los Estados Unidos para facilitar

[21] *Cfr.* las enmiendas incorporadas en el Informe A9-0256/2020 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (Comisión LIBE), ponente Birgit Sippel, disponible en: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_ES.html (fecha de consulta: 15/04/2025).

[22] *Vid.* sobre la relevancia de la *U.S. Cloud Act* y los prestadores de servicios estadounidenses, entre otros, Stanislaw Tosza (2020). "All evidence is equal…", *cit.*, 170. El desarrollo tecnológico conlleva que se abandone el enfoque el principio de territorialidad tradicional siendo irrelevante la ubicación de los datos, lo cual puede provocar que los proveedores entren en conflicto con la legislación de terceros Estados como Estados Unidos (176); Carrera, Sergio, Marco Stefan y Valsamis Mitsilegas (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,* Bruselas, Centre for European Policy Studies, 28-35. Conforme a la legislación estadounidense actualmente los proveedores únicamente proporcionan voluntariamente datos sin contenido, siendo necesario un nuevo marco regulador que incluiría otras categorías de datos, incluyendo los datos de contenido.

el acceso transfronterizo a la prueba electrónica, lo cual conllevaría un nada desdeñable avance hacia un nuevo sistema de cooperación de carácter global en materia de obtención de prueba electrónica. Sin embargo, dichas negociaciones no han progresado desde hace años, continuando en curso en la actualidad. De forma simultánea se otorgó un mandato para negociar con el Consejo de Europea el nuevo Protocolo adicional al Convenio de Budapest sobre la ciberdelincuencia, el cual fue adoptado en 2021 autorizándose su ratificación a los Estados miembros en 2023[23].

Consideramos que, dada la idiosincrasia de los datos electrónicos, la fórmula más adecuada para la obtención transfronteriza de la fuente de prueba electrónica, sería el sistema de transmisión directa de las órdenes a los prestadores de servicios por parte de las autoridades judiciales. Constituiría además un indudable avance en el ELSJ y en la consolidación de la confianza mutua entre los Estados miembros, que las autoridades judiciales de un Estado específico pudieran obtener la fuente de prueba electrónica de forma transfronteriza en la UE, de forma similar a un procedimiento interno. Ello en lugar de preterir o conculcar los avances en materia de cooperación judicial precisamente los fortalecería. Éste sería el cauce idóneo, dadas las vanguardistas técnicas utilizadas por la delincuencia en el ciberespacio, la relevancia que han adquirido los datos electrónicos en toda su extensión y los procedimientos lentos y anquilosados que actualmente tienen a su disposición las autoridades judiciales. Está por determinar si las nuevas órdenes, resultado del lento y complejo procedimiento legislativo referido, serán finalmente suficientes para la responder a las enormes dimensiones del reto enfrentado. Y ello dado que el imparable progreso tecnológico conlleva una rápida obsolescencia técnica de los propios sistemas y que aún tendremos que esperar a la efectiva praxis de estos nuevos instrumentos legislativos para poder valorar y comprobar su eficacia y efectividad real.

[23] *Vid*. https://www.consilium.europa.eu/es/policies/e-evidence/ (fecha de consulta: 15/04/2025). En el mandato para negociar con Estados Unidos se consideran especialmente los conflictos legales, las obligaciones contradictorias y las reglas comunes para la transferencia directa y recíproca de la prueba, con un sistema de garantías para proteger los derechos fundamentales. *Cfr*. https://www.consilium.europa.eu/es/meetings/jha/2019/06/06-07/ (fecha de consulta: 15/04/2025).

2. LA ORDEN EUROPEA DE PRODUCCIÓN

La OEP constituye una decisión emitida o validada por una autoridad judicial de un Estado miembro, por la que se ordena a un prestador que ofrezca en la UE 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, a que entregue la fuente de prueba electrónica con independencia de donde se ubiquen los datos. El EPOC se dirigirá directamente al establecimiento designado o a un representante legal del prestador de servicios[24]. Como hemos visto, no se permite la obtención de datos en tiempo real, es decir, como forma de prevención de la delincuencia o investigaciones prospectivas, constituyendo la fuente prueba electrónica los datos almacenados por el prestador de servicios o en su nombre cuando reciba el EPOC. El ámbito de aplicación de la OEP del mismo modo que de la OEC se limita exclusivamente a los procesos penales[25], incluyéndose la ejecución de penas o medidas de seguridad privativas de libertad con una duración de al menos cuatro meses si no fueron dictadas en rebeldía, límite penológico *a quo* que constituye una manifestación del principio de proporcionalidad, excluyéndose de forma expresa los procesos que se inicien para prestar asistencia judicial mutua a otro Estado miembro o país tercero[26].

El EPOC (Anexo I) será cumplimentado por la autoridad competente para la emisión o validación de la OEP, que lo firmará y certificará, transmitiéndolo a través de un sistema informático descentralizado compuesto por los sistemas informáticos de los Estados miembros y los órganos y organismos de la Unión, con puntos de acceso

[24] *Cfr. et al*, arts. 1.1, 2.2, 3.1, 3.3, 3.4, 7.1 y considerando nº 50 del Reglamento e-evidence.
[25] Para la interceptación de las telecomunicaciones o la investigación de ilícitos administrativos, el instrumento adecuado sería la OEI, respecto al cual la OEP desde esta perspectiva, presenta notables diferencias en su ámbito de aplicación.
[26] *Cfr.* art. 2.2 y 2.4 del Reglamento e-evidence.

interoperables basados en el sistema e-CODEX, el cual ha sido integrado en la totalidad de los instrumentos de cooperación judicial en la UE[27].

Las autoridades competentes y los límites penológicos *a quo* para la emisión de la OEP, son diferentes en función de las categorías específicas de datos conforme al principio de proporcionalidad. Si se trata de datos de abonados y de datos solicitados con la única finalidad de identificar al usuario, podrá emitirse respecto a todas las infracciones penales y para la ejecución de penas o medidas de seguridad con una duración mínima de cuatro meses, por un Juez, Tribunal, Juez de Instrucción, Fiscal u otra autoridad definida como autoridad de investigación por el Estado emisor, si bien en este último caso deberá validarse por un Juez, Tribunal, Juez de Instrucción o Fiscal. Cuando la OEP verse sobre datos de tráfico o de contenido, será necesario que los hechos punibles estén conminados con al menos tres años de privación de libertad en el Estado emisor, adquiriendo además relevancia la tradicional lista de treinta y dos delitos en los que no se efectuará el control de la doble tipificación (Anexo IV Reglamento e-evidence) o bien, que se trate de determinadas infracciones penales cometidas parcial o totalmente a través de un sistema de información. En estas categorías de datos las autoridades

[27] *Vid.* arts. 9, 19, considerando nº 83 *et at*, del Reglamento e-evidence. Inicialmente no se hacía referencia en la propuesta de Reglamento al sistema e-CODEX, aludiéndose únicamente a cualquier medio seguro que permita constancia escrita y de la autenticidad o bien, plataformas especializadas creadas *ad hoc* (art. 8.2 propuesta de Reglamento e-evidence). Obviamente es ineludible que el sistema informático descentralizado se base en el sistema e-CODEX, dada la plena integración de este sistema creado por el Reglamento (UE) 2022/850, relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX) (ELI: http://data.europa.eu/eli/reg/2022/850/oj), a través del Reglamento (UE) 2023/2844, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales (ELI: http://data.europa.eu/eli/reg/2023/2844/oj). Respecto al sistema e-CODEX y su relevancia en la digitalización de la cooperación judicial en la UE, véase Tinoco Pastrana, Ángel (2024): "Capítulo II. La evolución digital de la cooperación judicial y del acceso a la Justicia en la Unión Europea", en M. Jimeno Bulnes y Á. Tinoco Pastrana (Dirs.). *El Derecho procesal civil y penal desde la perspectiva de la Unión Europea: la consolidación del Espacio de Libertad, Seguridad y Justicia*, Valencia, Tirant lo Blanch. 136-146.

de emisión son las mismas que en las primeras exceptuándose al Fiscal, si bien siempre tendrá que validar la OEP un órgano jurisdiccional[28].

Se diferencian los tipos de infracciones penales y las autoridades de emisión en estos dos grupos de categorías de datos con distintos niveles de protección, dado que las medidas que versen sobre los segundos son de mayor carácter invasivo o coercitivo, lo cual ha sido considerado como un sistema de "geometría variable"[29]. En principio se puede considerar que ello estaría 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 es necesario el "control por una autoridad administrativa independiente" para la transferencia de los datos[30]. Conforme a los principios de necesidad y proporcionalidad[31], la OEP sólo podrá emitirse si en el Estado emisor está prevista una medida análoga en las mismas condiciones que en un asunto nacional similar (art. 5.2 Reglamento e-evidence), lo cual refleja la denominada "cláusula de cortesía internacional", evitándose de este modo el *forum shoping* probatorio dada la ausencia de armonización legislativa en la materia[32].

La tutela judicial efectiva se garantiza con el reconocimiento del derecho al recurso efectivo de la persona cuyos datos hayan sido solicitados, en el proceso penal el que se utilicen sus datos. Este derecho se ejercerá ante un órgano jurisdiccional del Estado emisor de la OEP

[28] *Vid.* arts. 4.1, 4.2, 5.3 y 5.4 del Reglamento e-evidence.

[29] Daniele, Marcelo: "L´acquisizione delle prove digitali dai service provider...", *cit.*, 1285-1287.

[30] En este sentido, 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.* 28 (4), 342-345. La primera categoría de datos es más adecuada para la identificación del investigado y la segunda, para la obtención de la prueba para el juicio oral; Carrera, Sergio, Marco Stefan y Valsamis Mitsilegas (2020). "Cross-border data Access in criminal proceedings…", *cit.*, 49, 57.

[31] Sobre la aplicación de estos principios, *vid.* Tinoco Pastrana, Ángel (2020). "The Proposal on Electronic Evidence in the European Union", *EUCRIM*. 1, 48-49.

[32] *Vid.* art. 5.2 del Reglamento e-evidence. *Cfr*. Geraci, Rosa Maria. (2019). "La circulazione transfrontaliera delle prove...", *cit.*, 1345 y Carrera, Sergio, Marco Stefan y Valsamis Mitsilegas (2020). "Cross-border data Access in criminal proceedings…", *cit.*, 59.

conforme a su legislación nacional, pudiendo impugnarse la legalidad, necesidad y proporcionalidad de la medida[33], de lo cual se informará en el momento oportuno a la persona afectada, al margen de las garantías de los derechos fundamentales en el Estado de ejecución y el respeto de los derechos de defensa y equidad en la valoración de la prueba electrónica obtenida. Se ha objetado respecto a la regulación de esta materia por el art. 18 del Reglamento e-evidence, que se realiza una referencia "muy sucinta" a "dos cuestiones de gran importancia", que deberían de recibir un tratamiento diferenciado: los recursos que se podrán interponer y las garantías en la admisibilidad y valoración de la prueba obtenida y que no está claro si podrán impugnar las órdenes las personas afectadas que no fueran ni investigados y acusados, lo cual debería concretarse en las legislaciones nacionales que desarrollen el Reglamento[34].

En cuanto a la ejecución del EPOC, tras su recepción el destinatario conservará los datos solicitados y los transmitirá de forma directa a la autoridad emisora o a las autoridades indicadas en el EPOC en un plazo máximo de diez días y ocho horas en casos urgentes, desde la recepción del EPOC, como hemos señalado. Si el destinatario estima que la ejecución del EPOC puede interferir con inmunidades o privilegios, normas sobre determinación de la responsabilidad penal en relación con la libertad de prensa o de expresión, informará a la autoridad emisora a través del Anexo III. A estos supuestos se añaden que el EPOC esté incompleto, contenga errores manifiestos o información insuficiente para su ejecución, o bien que surja una imposibilidad por causas ajenas a la voluntad del destinatario[35].

[33] *Cfr.* la información al usuario y confidencialidad regulada en el art. 13 del Reglamento e-evidence, en virtud del cual se informará sobre las vías de recurso disponibles, si bien la autoridad emisora de forma motivada podrá demorar, restringir e incluso omitir esta información.

[34] En este sentido, De Hoyos Sancho, Montserrat (2024): *La nueva regulación en la Unión Europea…*, *cit*., pp. 89-92.

[35] *Cfr.* art. 10.1 del Reglamento e-evidence y de forma más específica en cuanto a los motivos de no ejecución del EPOC por el destinatario, art. 10.5-7.

Junto a estos motivos concretos se incluye una "causa residual" que justificaría la no entrega de los datos por parte del destinatario del EPOC, hasta que las autoridades de emisión y ejecución en su caso, adopten una decisión específica al respecto. Se trata de que el destinatario alegue cualquier otra causa por la cual no puede facilitar los datos en el plazo establecido, lo cual deberá comunicar a la autoridad de emisión y en su caso a la de ejecución si fue notificada conforme al art. 8 a través del Anexo III. La autoridad emisora examinará el EPOC y en su caso, fijará un nuevo plazo para la entrega de los datos por el destinatario. En el Reglamento no se proporciona de forma clara una solución a esta situación, existiendo una previsión incompleta de esta "causa residual" por la cual la autoridad emisora podrá estimar que está justificado el incumplimiento y en consecuencia retirar la OEP, o bien considerar que existe un incumplimiento injustificado e iniciar el procedimiento de ejecución y el sistema sancionador[36].

Éstos constituyen los motivos de denegación generales para todas las OEP (art. 10), pero cuando la OEP verse sobre datos de tráfico y de contenido, la cual se notificará de forma obligatoria a la autoridad del Estado de ejecución, en el art. 12 del Reglamento e-evidence junto con los motivos que acabamos de referir se incorporan otros adicionales y específicos. A todo ello se añade el "reexamen en caso de obligaciones en conflicto" (art. 17) aplicable a la totalidad de las OEP. En conclusión, los motivos de denegación son más amplios cuando el EPOC versa sobre datos de tráfico y de contenido, como veremos en el estudio de esta modalidad.

Observamos que en la práctica puede suponer una gran dificultad para los prestadores de servicios efectuar la verificación legal de la OEP en plazos tan reducidos y, que a pesar de las indudables ventajas del sistema de cooperación público-privada creado éste no constituye un sistema exento de riesgos, ya que los prestadores de servicios constituyen

[36] *Vid.* Fuentes Soriano, Olga (2024). "Prueba penal transfronteriza: la normativa *«e-evidence»* como complemento de la orden europea de investigación", en C. Arangüena Fanego y M. de Hoyos Sancho (Dirs.). *Hacia un Derecho Procesal Europeo. IX Memorial Manuel Serra Domínguez*, Barcelona, Atelier. 149.

empresas privadas cuyo principal y legítimo objetivo consiste en obtener beneficios económicos. Por ello se ha llamado la atención sobre los peligros de encomendar a empresas privadas el control sobre la ejecución, lo cual puede conllevar la "privatización de la tutela de los derechos fundamentales"[37]. Está por comprobar cómo los prestadores de servicios sopesarán los múltiples intereses que están en juego y los deberes legales para cumplir con su función en la práctica. De hecho, el sistema sancionador respecto al incumplimiento de las obligaciones de ejecución por el destinatario del EPOC y de la obligación de confidencialidad (art. 15 Reglamento e-evidence), prevé junto a las sanciones penales previstas en los ordenamientos nacionales, sanciones pecuniarias que deberán ser "eficaces, proporcionadas y disuasorias", con el máximo del dos por ciento del total del volumen anual de negocios mundial del ejercicio precedente del prestador de servicios. Ello podría conllevar que los prestadores se conviertan en "receptores pasivos" de las órdenes, encontrándose en la obligación de ejecutarlas incluso cuando no debieran hacerlo[38]. Este sistema de pecuniario sancionador tan elevado, refleja que las instituciones europeas quieren garantizarse la máxima eficacia del sistema de obtención transfronteriza de la prueba electrónica y colaboración de los prestadores de servicios. Por ello se prevé la ejecución forzosa del EPOC (art. 16 Reglamento e-evidence) cuando el prestador no cumpliera, a través del cual la autoridad emisora podrá solicitar a la autoridad de ejecución que lo ejecute en un plazo de cinco días adoptando de forma inmediata las medidas necesarias para ello[39].

---

[37] Entre otros, Daniele, Marcelo (2019). *"L´acquisizione delle prove digitali dai service provider..."*, *cit*., 1288-1293. Ello no constituye una particularidad de este sistema europeo, existiendo un mecanismo similar en la *U.S. Cloud Act*, por lo que estaríamos ante una tendencia que se está imponiendo a nivel global; Mitsilegas, Valsamis (2018). "Cross-border data Access in criminal proceedings…", *cit.*, 265, que igualmente alerta de dichos riesgos y de que ello 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.

[38] Al respecto, Carrera, Sergio, Marco Stefan y Valsamis Mitsilegas (2020). "Cross-border data Access in criminal proceedings…", *cit.*, 60.

[39] *Vid.* De Hoyos Sancho, Montserrat (2024): *La nueva regulación en la Unión Europea…*, *cit*., pp. 75-76.

Respecto a la OEP referida a datos de tráfico y de contenido se incorpora junto a la notificación al destinatario del EPOC, la notificación obligatoria a la autoridad competente del Estado de ejecución, como hemos reiterado. Ello en gran medida, es consecuencia de la presión ejercida al respecto por la Comisión LIBE del Parlamento Europeo durante el procedimiento legislativo, donde uno de los puntos más controvertidos fue precisamente dicha notificación simultánea a la autoridad del Estado de ejecución[40], como hemos visto. No obstante, la notificación a la autoridad de ejecución posee las excepciones de que el delito se haya cometido, se esté cometiendo o se vaya a cometer en el Estado emisor y que la persona cuyos datos se soliciten resida en dicho Estado. En estos supuestos existe una "sólida y sustancial" vinculación de la causa al Estado emisor, por lo que el EPOC se ejecutaría como si versara sobre datos de abonados o de identificación del usuario, por lo que estamos de acuerdo en concluir que en la mayoría de los casos realmente no supervisaría el EPOC la autoridad del Estado de ejecución, por lo cual en la práctica serán muy limitadas las posibilidades que tendrían los prestadores de servicios de controlar realmente los motivos de denegación[41].

La notificación del EPOC a la autoridad de ejecución suspenderá las obligaciones del destinatario excepto en los casos de urgencia, definidos como aquellos en los que existe una amenaza inminente para la vida, integridad física, seguridad de la persona o una infraestructura esencial[42]. Esta notificación permite que la autoridad de ejecución dentro del plazo de diez días y de noventa y seis horas en caso de urgencia[43] desde

[40] En este sentido, además, Tosza, Stanislaw (2024). "Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights". *Common Market Law Review*, 61 (1), 149.

[41] *Vid.*, entre otros, De Hoyos Sancho, Montserrat (2024): *La nueva regulación en la Unión Europea…*, *cit.*, 55-56 y Tosza, Stanislaw (2024). "Mutual Recognition By Private Actors In Criminal Justice?...", *cit.*, 150.

[42] *Cfr.* arts 8.4 y 3.18 del Reglamento e-evidence.

[43] En casos urgentes, la transmisión tendrá lugar con carácter general en un plazo máximo de ocho horas. Pero si es necesario notificar a la autoridad de ejecución porque se trate de datos de tráfico o de contenido, el plazo que tendrá dicha autoridad para invocar un motivo de denegación será de noventa y seis horas. Si la autoridad invoca un motivo de denegación y los datos ya han sido transmitidos a la autoridad emisora, ésta tendrá que

la recepción del EPOC, lo controle para verificar si concurre algún motivo de denegación del art. 12[44]. Éstos consisten en que los datos estén protegidos por privilegios o inmunidades, o bien estén cubiertos por normas relativas a la determinación de la responsabilidad penal relacionadas con la libertad de prensa o de expresión, los cuales coinciden con los previstos en el artículo 10.5, a los que se añade en el art. 12 que la ejecución pueda vulnerar de forma manifiesta un derecho fundamental, sea contraria al principio *non bis in ídem* o que la conducta no sea constitutiva de delito en el Estado de ejecución y no conste en la lista de treinta y dos delitos en los que no se efectuará el control de la doble tipificación del Anexo IV, punibles en el Estado emisor con una pena o medida de seguridad de al menos tres años de duración.

Estos motivos adicionales de denegación a los del art. 10.5 como hemos avanzado, no están previstos para cuando el prestador de servicios sea el único destinatario del EPOC, por tanto, cuando verse sobre datos de abonados y datos solicitados con el único fin de identificar al usuario. Antes de que la autoridad de ejecución invoque un motivo de denegación deberá consultarlo con la autoridad de emisión, la cual podrá adaptar o retirar la OEP. Si finalmente la autoridad de ejecución invoca un motivo de denegación informará al destinatario y a la autoridad de emisión. El destinatario interrumpirá la ejecución y la autoridad emisora retirará la orden. También es posible que la autoridad de ejecución cuando invoque un motivo de denegación se oponga a la transferencia de los datos

suprimirlos o restringir su uso o bien utilizarlos conforme a las condiciones indicadas por la autoridad de ejecución (art. 10.4 Reglamento e-evidence). Este mecanismo y solución es análoga incluso en el plazo, a la Intervención de las telecomunicaciones sin la asistencia técnica del "Estado notificado" en la DOEI (art. 31.3 DOEI), a la cual nos referimos anteriormente, que como vimos no constituye una OEI en sentido estricto, aunque entre dentro del ámbito de aplicación de la DOEI.

[44] Los motivos de denegación de este precepto constituyen "motivos de denegación inicial", excluyendo la posibilidad de que se invoquen los del procedimiento de ejecución, contemplados en el art. 16, que coinciden parcialmente con aquellos, lo cual aumenta la complejidad del sistema de ejecución del Reglamento e-evidence. En este sentido, *vid.* Gómez Amigo, Luis (2024). "Estudio de las órdenes europeas de producción y conservación: un instrumento eficaz para la obtención transfronteriza de pruebas penales electrónicas". *Revista Española de Derecho Europeo.* 92, 81.

solicitados, o bien que indique que éstos únicamente se podrán transferir o utilizar parcialmente en las condiciones que establezca dicha autoridad. Si la autoridad de ejecución antes de la finalización del referido plazo de diez días no invoca ningún motivo de denegación, el destinatario del EPOC actuará lo antes posible y a más tardar, al final del plazo de diez días[45].

Otras incidencias en la ejecución están previstas bajo la rúbrica de "reexamen en caso de obligaciones en conflicto" (art. 17 Reglamento e-evidence). Cuando el destinatario considere que la ejecución de la OEP entre en conflicto con la legislación de un tercer Estado, informará igualmente a través del Anexo III con la consiguiente obligación de conservar los datos, lo cual se contempla como "objeción motivada", que se podrá plantear en el plazo de diez días y que no se podrá fundamentar en que en la legislación del tercer Estado no concurran similares disposiciones sobre la emisión de la OEP ni en que los datos estén almacenados en un tercer Estado. Esta cuestión previsiblemente tendrá una notable relevancia en el funcionamiento del *e-evidence package*, dada la necesidad de resolver los conflictos que surjan a los prestadores de servicios con sede en otros Estados, sobre todo fuera de la UE[46]. El procedimiento de reexamen es fundamental, ya que en la actualidad dado el desarrollo tecnológico y el uso de la "nube informática" se tiende a

[45] *Cfr*. arts. 10.2 y 12.2-4 del Reglamento e-evidence.

[46] De Hoyos Sancho, Montserrat (2024): *La nueva regulación en la Unión Europea…*, *cit.*, 81-87. El legislador europeo incluyó esta previsión, considerando los conflictos de normas y obligaciones que se les pueden plantear a los prestadores de servicios norteamericanos con sede en la UE. La *US Cloud Act* establece que estos prestadores tendrán que cumplir con la legislación norteamericana para entregar los datos, con independencia de donde se almacenen. Se prevé que para cuando las solicitudes de entrega provengan de autoridades extranjeras, Estados Unidos pueda firmar "acuerdos ejecutivos" con gobiernos extranjeros. Hasta el momento, únicamente se han firmado dos acuerdos de este tipo, siendo en este sentido importante el acuerdo ejecutivo que la UE está negociando con Estados Unidos, el cual como vimos lleva años en curso. Ello supone que las obligaciones al respecto de los prestadores norteamericanos, dependerán de la aplicación del 2º Protocolo Adicional al Convenio de Budapest sobre Cibercrimen. Por ello no es aventurado afirmar, que cuando sea aplicable el *e-evidence package*, tanto las autoridades de emisión y ejecución como los prestadores de servicios, no tendrán una situación precisamente "sencilla".

abandonar el enfoque el principio de territorialidad tradicional, que vincula la jurisdicción con el lugar donde se almacenen los datos[47].

3. LA ORDEN EUROPEA DE CONSERVACIÓN

A través de la OEC se ordena al establecimiento designado o al representante de un prestador de servicios que los ofrezca en la UE cuando reciba el certificado EPOC-PR, a la conservación de pruebas electrónicas para que éstas puedan entregarse posteriormente a través de la OEP, OEI o de la asistencia judicial, impidiéndose la retirada, supresión o alteración de los datos[48]. La OEC coincide con la OEP tanto la definición de autoridad emisora como la de prestador de servicios, entre otros muchos aspectos, diferenciándose fundamentalmente en la finalidad.

Las diferencias estriban en que la determinación de la autoridad emisora no se establece en función de la categoría específica de datos sobre la que verse la OEC, dado que son las mismas autoridades respecto a todas, coincidiendo con las establecidas en la OEP respecto a los datos de abonados y datos solicitados con el único fin de identificar al usuario. En consecuencia la OEC puede emitirse en la totalidad de los supuestos por un Juez, Tribunal, Juez de Instrucción, Fiscal o cualquier autoridad competente definida por el Estado emisor que actúe como autoridad de investigación en procesos penales[49]. También existen diferencias en las condiciones para la emisión de la OEC que redundan en su sistema de garantías, las cuales son más sucintas que las establecidas para la OEP. La OEC deberá responder a los principios de necesidad y proporcionalidad, pudiéndose emitir respecto a todas las infracciones penales, al igual que respecto a la ejecución de una pena o medida de seguridad privativa de libertad, con duración mínima de cuatro meses, en todas las categorías de

[47] Sobre dicho enfoque, *vid.* Tosza, Stanislaw (2020). "All evidence is equal…", *cit.*, 176; Daniele, M. (2019): "L´acquisizione delle prove digitali dai service provider...", *cit.*, 1290-129, que resalta el importante papel de los prestadores de servicios en la valoración de la existencia del conflicto legal, aunque su conducta podría condicionarse por el interés en mantener una buena relación con el Estado en el que ejercen su actividad.
[48] *Vid.* arts. 3.2 y 6.2 del Reglamento e-evidence.
[49] *Vid.* art. 4.3 del Reglamento e-evidence.

datos[50], condiciones que coinciden con la OEP referida a datos de abonados y de identificación, del mismo modo que las autoridades de emisión, como acabamos de señalar.

En consecuencia, las pruebas electrónicas conservadas a través de la OEC que versen sobre datos de tráfico y de contenido únicamente podrán ser entregadas a través de la OEP si se cumplen las condiciones estudiadas *ut supra*, dados los diversos requisitos de la OEP y OEC respecto a las diversas categorías de datos. Si la entrega no es posible a través de la OEP deberá acudirse a otras vías como, por ejemplo, la OEI o la asistencia judicial mutua. Consideramos que en la práctica puede ser más frecuente e incluso útil la conservación de los datos a través de la OEC que la propia OEP, dada la interacción de la primera con los otros mecanismos diferentes para la entrega de los datos, además de que cuando no se ejecute la OEP ésta quedará en gran medida subsumida en una OEC, al conllevar la inmediata conservación de los mismos. No debemos olvidar la importancia de preservar los datos, dados los riesgos de volatilidad, destrucción y facilidad de su ocultación, por lo que es fundamental la adecuada conservación y preservación de la "cadena de custodia digital".

La información o contenido que deberá incluir la OEC coincide sustancialmente con la de la OEP. En cuanto a la ejecución de la OEC, la transmisión al destinatario se efectuará a través del EPOC-PR, que de la misma forma que el EPOC cumplimentará la autoridad emisora o validadora. Tras la recepción del EPOC-PR el destinatario deberá conservar sin demoras los datos durante un plazo máximo de sesenta días, prorrogables por otros treinta. Si tras este período se emite una posterior solicitud de entrega, el destinatario tendrá que conservar los datos durante el tiempo necesario para ello[51]. Ya que la entrega se puede producir a través de diversos mecanismos como hemos visto (OEP, OEI o asistencia judicial mutua), en realidad el período máximo de conservación no deja de estar indeterminado. Por ello se debe llamar la atención respecto a la falta de salvaguardias en relación a la conservación general e indiscriminada de

[50] *Vid*. art. 6.1-.3 del Reglamento e-evidence.
[51] *Cfr*. art. 11.1 del Reglamento e-evidence.

los datos, conforme a la jurisprudencia del TJUE (asuntos acumulados *Tele2 Sverige AB v. Post-ochtelestyrelsen*)[52]. La autoridad emisora tendrá que informar a la mayor brevedad cuando la conservación ya no fuera necesaria. Si surgieran incidencias que impidieran que el destinatario cumpliera su obligación, porque el EPOC-PR esté incompleto, tenga errores o no incorpore la suficiente información para ejecutarlo, informará sin demora a la autoridad de emisión a través del Anexo III. Del mismo modo el destinatario informará tanto a la autoridad de ejecución como a la de emisión, en el supuesto específico de que la ejecución del EPOC-PR, interfiriera con inmunidades o privilegios, libertad de prensa o de expresión en el Estado de ejecución, a través del Anexo III[53].

En la OEC posee plena aplicación, el régimen de confidencialidad e información al usuario en los mismos términos que en la OEP, del mismo el sistema de sanciones y el régimen del incumplimiento del EPOC-PR por el destinatario. La diferencia fundamental estriba en que respecto a la OEC no se contemplan las vías de recurso efectivas previstas para la OEP[54] y en los motivos de denegación de la OEC, los cuales son significativamente más sucintos que en la OEP. En definitiva, parece que el legislador europeo ha prestado más atención a la OEP que a la OEC, lo cual refleja en que el sistema de garantías de ésta sea inferior, lo cual consideramos que debería haberse solventado en el texto definitivo. Como hemos señalado la conservación de los datos podrá llegar a ser tan relevante en la práctica

[52] Al respecto, Rogalski, M. (2020). "The European Commission´s e-Evidence Proposal…", *cit.*, 348-349. El período de conservación no se define de forma inequívoca conforme a la jurisprudencia del Tribunal de Justicia de la Unión Europea.

[53] *Cfr.* art. 11.4 y .5 del Reglamento e-evidence.

[54] De Hoyos Sancho, Montserrat (2022). "Reflexiones acerca de la propuesta de Reglamento UE…", *cit.*, 22. Considera que ello pone de manifiesto que la propia Comisión en la propuesta de Reglamento consideró de menor intensidad la intromisión en los derechos fundamentales de la persona afectada por la OEC, advirtiendo que es probable que los Estados incorporen en sus propias normas medios de impugnación que incluyan las órdenes de conservación. En este sentido, Gómez Amigo, Luis (2024). "Estudio de las órdenes europeas de producción y conservación…", *cit.*, 85, cuestiona igualmente esta exclusión de las vías de recurso efectivas en la OEC y considera del mismo modo que conforme al Derecho nacional éstas podrán crearse, de conformidad con lo previsto en el art. 18.1 del Reglamento e-evidence.

como la propia entrega e incluso superior, siendo en todo caso prioritario que se realice de forma correcta, lo cual permitiría conseguir la posterior admisibilidad probatoria. Los datos conservados podrán entregarse a través de vías diferentes a la OEP, como la OEI o la asistencia judicial, creándose una forma lógica interacción de este nuevo instrumento con los ya existentes como hemos visto, lo cual creemos que debería haber recibido una mayor atención legislativa. Y ello salvo que de lo que se trate realmente, sea precisamente ello es decir, de permitir sobre todo la conservación de los datos a toda costa, dada su volatilidad y facilidad de ocultación y las propias dificultades operativas que puedan surgir con la ejecución de la OEP, si bien reiteramos que no podemos defender ningún tipo de conservación de datos de carácter indiscriminado sin límites claros y garantías precisas, que puedan conculcar los derechos fundamentales y poner en riesgo los derechos fundamentales y más concretamente, el invocado "derecho al entorno virtual". No obstante, del mismo modo que hemos dicho respecto a la OEP, únicamente la efectiva práxis de las nuevas órdenes, además de los controles jurisdiccionales que se ejerzan por las autoridades judiciales, responsables y garantes de los derechos fundamentales de la ciudadanía, serán los elementos fundamentales que nos permitan, entre otros, poder valorar tanto la eficacia como el respeto de los derechos fundamentales y garantías procesales, por las OEP y OEC.

4. CONCLUSIONES

La creación de un instrumento para la obtención y conservación de la prueba electrónica transfronteriza en los procesos penales, constituye sin duda una necesidad apremiante en el ELSJ. La UE no puede estar al margen del imparable desarrollo tecnológico, de la relevancia que en la actualidad poseen los datos electrónicos en toda su extensión para la investigación y enjuiciamiento de los delitos y del importante papel que al respecto poseen los prestadores de servicios de comunicaciones electrónicas y de la sociedad de la información. Del mismo modo, la UE tampoco puede eludir las dificultades que en la actualidad en esta materia enfrentan las autoridades nacionales, la realidad existente a nivel global, la necesidad inherente a la fuente de prueba electrónica de cooperar con

terceros Estados dado su almacenamiento fuera de la UE, facilidad de ocultación y destrucción y, los mecanismos que se han creado respecto la obtención de la prueba electrónica en otros países como Estados Unidos, el cual adquiere un especial protagonismo en esta materia.

Por ello destacamos como el aspecto fundamental del Reglamento e-evidence y en consecuencia de las OEP y OEC, la creación del nuevo modelo de cooperación directa público-privada entre las autoridades de emisión y los prestadores de servicios, el cual como hemos visto en absoluto ha estado exento de polémica, habiendo tensionado el lento y arduo procedimiento legislativo para la adopción del Reglamento e-evidence y la Directiva sobre representantes legales y establecimientos designados de los prestadores de servicios.

Pero creemos que este modelo lejos de conculcar los avances logrados en el ELSJ a través de los clásicos instrumentos de reconocimiento mutuo, incluso los consolida, dado el alto grado de confianza mutua entre los Estados miembros que requieren las nuevas órdenes europeas, confianza mutua que se fortalecería por lo innovador que resulta que una autoridad pueda obtener la fuente de prueba electrónica en otro Estado, como si se tratara de un procedimiento interno. Consideramos en definitiva que el modelo de transmisión directa de las órdenes a los prestadores de servicios sería el modelo adecuado e idóneo, para la obtención transnacional de la prueba electrónica. Las simetrías que este modelo posee con la *US Cloud Act* norteamericana precisamente facilitaría la creación de un sistema de obtención e intercambio de prueba electrónica a nivel global, que permitiría evolucionar al Derecho europeo y avanzar en la creación de normas homogéneas en materia de exclusión probatoria, solventando la actual fragmentación de la normativa procesal en la UE sobre la obtención y admisión de la prueba en los Estados miembros. El nuevo sistema de transmisión directa de las órdenes introduce una notable e imprescindible simplificación procedimental respondiendo a la necesidad acuciante al respecto, intenta dar respuesta a la naturaleza específica de los datos electrónicos, además de mejorar significativamente a través de la Directiva (UE) 2023/1544 la interlocución entre las autoridades estatales y los prestadores de servicios cuando ofrezcan sus servicios en la UE, de lo cual se beneficia además tanto el sistema de asistencia judicial como la OEI y los propios procedimientos penales internos.

Pero estas conclusiones o reflexiones no implican que no podamos cuestionar tanto el Reglamento e-evidence como la propia Directiva (UE) 2023/1544. Son numerosos los aspectos que hemos advertido que

consideramos deberían haber requerido una mayor atención legislativa o bien que no están lo suficientemente claros en los textos legislativos promulgados, los cuales hemos tratado a lo largo de este trabajo, del mismo modo que los retos enfrentados que aún están por lograr. Por ejemplo, el imprescindible Acuerdo entre la UE y los Estados Unidos para facilitar el acceso transfronterizo a la prueba electrónica, cuya negociación lleva años en curso y sería fundamental para la operatividad de la totalidad del sistema creado por el Reglamento e-evidence. Son cuestionables por ejemplo y sin ser exhaustivos, la falta de claridad de la regulación del reconocimiento del derecho a un recurso efectivo por la persona cuyos datos se han solicitados, la carencia de homogeneidad y claridad de los motivos de denegación de la OEP en función de las categorías de datos específicas y la necesidad de notificación a la autoridad de ejecución, los diferentes estándares de garantías procesales que existen entre la OEP y la OEC, la falta de claridad en ésta del plazo máximo de conservación o la ausencia de la regulación de las vías de recurso. Incluso consideramos cuestionable que finalmente se incorporara la notificación obligatoria a la autoridad de ejecución en los datos de tráfico y de contenido, dado que pueden existir otros mecanismos y controles diferentes que permitan que las nuevas órdenes sean realmente eficaces, sin obstaculizar o desnaturalizar el procedimiento que sería más adecuado. Estamos sin duda ante un cambio de mentalidad en materia de obtención transnacional de la prueba en la UE que puede constituir un indudable progreso. Pero ello nunca debe conllevar poner en riesgo o conculcar el sistema de garantías procesales del acervo normativo de la UE, siendo fundamental la aplicación del principio de proporcionalidad para asegurar la coherencia de todo el sistema y poner en valor la libertad y la justicia en el ELSJ, el cual está dominado por la seguridad, de lo cual obviamente no es responsable el nuevo Reglamento e-evidence, puesto que también al respecto podrían ser cuestionables los tradicionales instrumentos de reconocimiento mutuo.

De todos modos, no sabemos si las nuevas órdenes serán realmente suficientes para responder a los importantes retos enfrentados, dado el imparable progreso tecnológico y que aún tendremos que esperar a la efectividad real de las nuevas órdenes para poder comprobar su eficacia y virtualidad, del mismo modo que los propios controles jurisdiccionales que se ejerzan por las autoridades judiciales como garantes de los derechos fundamentales y las garantías procesales de la ciudadanía. En definitiva, si bien las nuevas órdenes europeas constituyen un indudable avance y

responden la acuciante necesidad existente en esta materia, aún debemos esperar para poder hacer balance y valorar con todos los elementos necesarios, el *e-evidence package*.

BIBLIOGRAFÍA

Carrera, Sergio, Marco Stefan y Valsamis Mitsilegas (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*, Bruselas, Centre for European Policy Studies, pp. 1-99.

Daniele, Marcelo (2019). "L´acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale". *Revista Brasileira de Direito Processual Penal*. 5 (3), pp. 1277-1295.

De Hoyos Sancho, Montserrat (2022). "Reflexiones acerca de la propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal". *Revista General de Derecho procesal*. 58, pp. 1-44.

De Hoyos Sancho, Montserrat. (2024). *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Analisis y valoración del "e-evidence package"*. Las Rozas. Aranzadi.

Forlani, Gianluca (2023). "The E-evidence Package. The Happy Ending of a Long Negotiation Saga". EUCRIM. 2, pp.174-181.

Fuentes Soriano, Olga (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 Olga Fuentes Soriano (Dir.), *Era digital, sociedad y Derecho*, Valencia, Tirant lo Blanch, pp. 281-320.

Fuentes Soriano, Olga (2024). "Prueba penal transfronteriza: la normativa *«e-evidence»* como complemento de la orden europea de investigación", en Coral Arangüena Fanego y Montserrat de Hoyos Sancho (Dirs.). *Hacia un Derecho Procesal Europeo. IX Memorial Manuel Serra Domínguez*, Barcelona, Atelier, pp. 219-260.

Geraci, Rosa Maria (2019). "La circulazione transfrontaliera delle prove digitali in UE: La proposta di Regolamento e-evidence". *Cassazione penale,* 59 (3), pp. 1340-1362.

Gómez Amigo, Luis (2024). "Estudio de las órdenes europeas de producción y conservación: un instrumento eficaz para la obtención transfronteriza de pruebas penales electrónicas". *Revista Española de Derecho Europeo.* 92, 43-91.

Mitsilegas, Valsamis (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*, 25 (3), pp. 263-265.

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.* 28 (4), pp. 333-353.

Stefan, Marco y Gloria González Fuster (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, November (updated in May 2019)*, Bruselas, Centre for European Policy Studies, pp. 1-70.

Sippel, Birgit (2023). "Guest Editorial". EUCRIM. 2, p. 109.

Tinoco Pastrana, Ángel (2020). "The Proposal on Electronic Evidence in the European Union", EUCRIM. 1, pp. 48-50.

Tinoco Pastrana, Ángel. (2021). "Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea". *Cuadernos de Política Criminal*. 135, pp. 203-246.

Tinoco Pastrana, Ángel (2024): "Capítulo II. La evolución digital de la cooperación judicial y del acceso a la Justicia en la Unión Europea", en Mar Jimeno Bulnes y Ángel Tinoco Pastrana (Dirs.). *El Derecho procesal civil y penal desde la perspectiva de la Unión Europea: la consolidación del Espacio de Libertad, Seguridad y Justicia*, Valencia, Tirant lo Blanch, pp. 121-159.

Tosza, Stanislaw (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*, 11 (2), pp. 171-183.

Tosza, Stanislaw (2024). "Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights". *Common Market Law Review*. 61 (1), pp. 139-166.