diariolaley

ARANZADI LA LEY

Luces y sombras del nuevo «paquete *e-evidence*» sobre obtención transfronteriza de pruebas electrónicas en procesos penales en la Unión Europea

Lights and Shadows of the New "E-Evidence Package" on the Cross-Border Acquisition of Electronic Evidence in Criminal Proceedings in the European Union

Montserrat de Hoyos Sancho

Catedrática de Derecho Procesal y exdirectora del Instituto de Estudios Europeos de la Universidad de Valladolid

LA LEY Unión Europea, Nº 149, Sección Tribuna, Julio 2026

ÍNDICE

Comentarios

I. Introducción (1)

Desde cualquier perspectiva de análisis, es evidente que las autoridades encargadas de la investigación y enjuiciamiento de los delitos necesitan disponer, cada vez en mayor medida, de cierta información electrónica que almacenan los proveedores de servicios de internet, que además tendrá que ser entregada por éstos de manera rápida y ciertamente segura. En muchos casos esos datos se encontrarán almacenados fuera de las fronteras donde se lleva a cabo la investigación policial o donde se tramita el proceso penal, por lo que será preciso hacer uso de los instrumentos de cooperación transfronteriza o de la asistencia mutua internacional, dependiendo de las circunstancias.

Los datos electrónicos más solicitados en las investigaciones penales hoy en día son los siguientes: información sobre el uso de aplicaciones de mensajería y correo electrónico —WhatsApp, Gmail y similares—, de redes sociales, sobre intercambio de criptomonedas, información almacenada «en la nube», datos sobre redes privadas virtuales (VPN), geolocalización de dispositivos, y acerca de compras y pagos *online* (2) .

Actualmente disponemos en el ámbito de la Unión Europea de un instrumento de cooperación transfronteriza, basado en el reconocimiento mutuo de resoluciones judiciales, que permite la obtención de este tipo de información y datos electrónicos almacenados en otro Estado de la Unión: la Orden Europea de Investigación (3) (OEI en lo sucesivo).

No obstante, si bien la aplicación de la Directiva 2014/41/CE (LA LEY 6702/2014), relativa a la orden europea de investigación en materia penal, implicó un avance muy importante en relación con las obtención transfronteriza de pruebas, y de hecho se utiliza constantemente con notable éxito, la OEI presenta muchas e importantes limitaciones cuando lo que se necesita es información electrónica almacenada por los proveedores de servicios de internet en otro Estado, por las siguientes razones: sigue siendo un instrumento de cooperación demasiado lento, e incluso en ocasiones se incumplen los plazos previstos en la norma, también en los casos urgentes; las pruebas electrónicas son muy volátiles, los datos pueden ser alterados e incluso borrados periódicamente, también de manera involuntaria; en muchos casos no se podrá saber dónde está concretamente la prueba en el momento en que la autoridad competente ha de cursar la petición, pues frecuentemente los datos se almacenan de forma

fraccionada, itinerante y/o en servidores fuera de la UE, por lo que será muy complicado determinar a qué concreta autoridad judicial se ha de dirigir la OEI (4) .

Por si todos estos no fueran suficientes inconvenientes, todavía a día de hoy, algunos de los proveedores de servicios más relevantes no tienen representación o delegaciones en el ámbito territorial de aplicación de la OEI que puedan dar respuesta a estas peticiones de entrega de información electrónica, por lo que en muchos casos habrá que emplear el todavía más lento y complejo instrumento de las clásicas «comisiones rogatorias» —*Mutual Legal Assistance, MLA*—, principalmente dirigidas a las autoridades de los Estados Unidos, donde están implantados importantes proveedores de servicios de internet, los que más peticiones reciben, como Google, Meta, X, Snapchat, Apple, Yahoo, Uber, LinkedIn, Reddit, etc.

La digitalización de las actividades económicas y sociales ha convertido la información electrónica en un elemento esencial de la investigación penal. Una parte creciente de las pruebas relevantes se encuentra almacenada por proveedores de servicios situados fuera del Estado que instruye el procedimiento

Hasta la fecha algunos de estos inconvenientes se vienen solventando, cuando es posible, recurriendo las autoridades nacionales competentes en cada supuesto a la llamada «cooperación voluntaria directa», que es la que pueden prestar los proveedores de servicios de internet cuando se les solicitan datos de abonados o incluso de tráfico, en ningún caso si se requieren datos de contenido.

Esta forma de cooperación directa es la que más se ha utilizado hasta ahora en la práctica (59% de las solicitudes), más incluso que la OEI (10%) (5) , pero se lleva a cabo en cierta medida de manera informal, pues si bien tal posibilidad se recoge en el art. 18 del Convenio de Budapest sobre cibercrimen (LA LEY 21666/2001) (6) —«*órdenes de presentación*»— y puede ampararse también en el Acuerdo de asistencia judicial entre la Unión Europea y EE UU (7) , esas «órdenes» a las que se refiere el Convenio no están reguladas detalladamente en los respectivos ordenamientos nacionales.

El panorama normativo y práctico *supra* descrito debería cambiar sustancialmente a partir del 18 de agosto de 2026, momento en el que tendría que estar plenamente operativo el conocido como «paquete *e-evidence*»: Reglamento (UE) 2023/1543 del Parlamento europeo y del Consejo, de 12 de julio de 2023 (LA LEY 22209/2023), 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, que va acompañado de la Directiva (UE) 2023/1544, del Parlamento europeo y del Consejo, de 12 de julio de 2023 (LA LEY 22208/2023), por la que se establecen normas armonizadas para la designación de establecimientos y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales (8) .

Lamentablemente, todo indica que nuestro país no llegará a tiempo a ese cambio, pues si bien el Reglamento es norma de aplicación directa en todos los Estados miembros (9) , en este supuesto es preciso aprobar una ley nacional que adapte los respectivos ordenamientos procesales a lo establecido en el Reglamento y, en todo caso, es imprescindible transponer la citada Directiva —lo que tenía que haber ocurrido antes del pasado 18 de febrero de 2026—, pues es la norma que obliga a los proveedores de servicios que operan en la Unión a designar establecimientos o representantes precisamente en el territorio UE, cuestión fundamental a estos efectos de solicitud de información electrónica.

En el momento en que se redactan estas líneas solo hemos tenido conocimiento de un Anteproyecto de Ley para la incorporación a nuestro ordenamiento interno de esa normativa UE, que fue presentado por el Ministerio de la Presidencia, Justicia y relaciones con las Cortes, junto con el Ministerio para la Transformación Digital y de la Función Pública, con fecha de marzo 2026 (10) . Como era previsible, se propone que esa legislación de adaptación, desarrollo y complemento se incardine en la *Ley 29/2014 (LA LEY 18182/2014), de reconocimiento mutuo de resoluciones penales en la Unión Europea* (11) ; concretamente, introduciendo una nueva Disposición Adicional octava.

Indicaremos a continuación, muy sucintamente, algunos de los aspectos más destacables de ese Anteproyecto desde el punto de vista orgánico y procesal (12) .

Dependiendo del tipo de datos solicitados al proveedor de servicios, serán autoridades de emisión de una «orden de producción/entrega» —EPOC (13) — las siguientes: el órgano jurisdiccional o el fiscal

competente en la causa si se pidieran datos de abonados o para la identificación de usuarios; solo el órgano jurisdiccional si se solicitaran datos de tráfico o de contenido. La policía podrá requerir sin validación previa y en caso de urgencia datos de abonados o de identificación de usuarios, y también podrá emitir «órdenes de conservación» —EPOC-PR (14) —, debiendo solicitar posteriormente y sin demora, en 48 horas, la validación por el órgano jurisdiccional competente (15) .

Será autoridad de ejecución en España a los efectos del Reglamento 2023/1543, la Sección de Instrucción del Tribunal de Instancia de Madrid. Le corresponderá también intervenir en caso de incumplimiento de las órdenes que reciban los proveedores de servicios y, en su caso, imponer la correspondiente sanción pecuniaria mediante resolución motivada (16) .

Por lo que respecta a los recursos —«vías de recurso efectivas» a las que se refiere el art. 18 del Reglamento—, el articulado del Anteproyecto prevé estos: contra el EPOC emitido por el órgano jurisdiccional competente, podrán interponerse recursos de reforma y apelación; si lo emitió el Ministerio Fiscal, podrá *impugnarse* en cinco días ante la Sección de Instrucción o de Menores del Tribunal de Instancia competente, y contra el auto resolutorio cabrá apelación; y lo mismo si lo emitiera un Fiscal Europeo Delegado.

También se concreta en nuestra ley nacional de transposición el régimen de infracciones y las consiguientes sanciones para los supuestos en que los proveedores de servicios incumplan las obligaciones y garantías que les impone la normativa europea.

II. Principales ventajas y oportunidades que ofrece el «paquete *e-evidence*»

Ha de valorarse positivamente el hecho de que por fin podamos disponer en el ámbito UE de una regulación común para la obtención de información electrónica almacenada por los proveedores de servicios de internet que actúan en el «espacio de libertad, seguridad y justicia» de la Unión Europea. Era imprescindible además que esa información electrónica que se necesita en una investigación penal se pudiera obtener de forma rápida y segura, pues resulta ser extremadamente frágil y volátil (17) .

La Orden Europea de Investigación no resultaba ser un instrumento suficientemente idóneo a estos efectos (18) , por su relativa lentitud y, sobre todo, porque si importantes prestadores de servicios de

internet no cuentan con establecimiento en la Unión a los efectos de cooperar con las autoridades nacionales europeas, muchas de las peticiones de datos que se les cursan se tendrán que seguir tramitando a través de «comisiones rogatorias» —*Mutual Legal Assistence, MLA*—, con todo lo que ello implica.

Ni el Convenio de Budapest de 2001, ni sus Protocolos adicionales, ni otros acuerdos, convenios o tratados bi- o multilaterales han podido dar solución hasta la fecha a todas las necesidades que se han puesto de manifiesto en esta materia. Tampoco la acción unilateral de los Estados miembros era la solución adecuada (19) .

Por otro lado, si bien desde hace mucho tiempo se viene haciendo uso de la mencionada cooperación voluntaria directa que prestan los proveedores de servicios *para obtener datos que no sean de contenido*, principalmente empresas establecidas en EE UU y como alternativa a las «comisiones rogatorias», con una eficacia notable (20) , esta cooperación directa entre autoridades nacionales y proveedores de servicios establecidos en otros Estados fuera de la Unión presenta también inconvenientes importantes, precisamente por la «voluntariedad» que sustenta esa cooperación. Falta en muchos casos el detallado soporte normativo de estas actuaciones, lo que siempre es un riesgo, también para la posterior utilización en la causa de la prueba en cuestión. Además, el éxito de la solicitud de cooperación depende de las respectivas políticas empresariales y de privacidad de cada uno de los proveedores, así como del cumplimiento por éstos de la legislación nacional del país donde tiene su establecimiento, que también les vincula y puede plantear inconvenientes que finalmente frustren la entrega de datos. En particular debe tenerse en cuenta la obligatoria aplicación de las estrictas reglas que en materia de cooperación con autoridades extranjeras se contienen en la *CLOUD Act* norteamericana (21) .

Es de suponer que con la entrada en funcionamiento del «paquete *e-evidence*» estos canales de cooperación voluntaria directa serán reemplazados por las «órdenes de producción» y «órdenes de conservación», pues *todos* los proveedores de servicios que presten servicios en la UE tendrán que tener establecimiento o al menos representación en algún Estado de la Unión en el que estén operando, y allí se les podrán dirigir estas órdenes de entrega o conservación de información electrónica, con lo

que se ganará en seguridad jurídica y fiabilidad de las pruebas remitidas a través de canales seguros de comunicación.

También puede considerarse una ventaja el hecho que las instituciones UE hayan optado por un conjunto normativo (Reglamento + Directiva) pues evitará disparidades relevantes entre las legislaciones de los Estados miembros sobre la materia.

Desde luego el Reglamento es un instrumento que ofrece ventajas importantes, como su aplicación directa y uniforme por los Estados miembros, lo que minimiza el riesgo de posibles interpretaciones divergentes por parte de las autoridades nacionales (22) .

Además, ha de ser valorada positivamente la superación en este ámbito del llamado *principio de territorialidad*, que se sustituye por el del lugar en que se ofrece el servicio —*Markortprinzip*—.

Desde el momento en que la información se almacena «en la nube», también en servidores fuera del espacio UE, o de manera itinerante, incluso fragmentadamente, no podemos seguir aplicando el principio de territorialidad —lugar en que se encuentra la prueba— para determinar la autoridad judicial competente que prestará la cooperación transfronteriza requerida.

Estimamos un acierto el cambio de modelo en relación con la obtención de este concreto tipo de fuentes de prueba. En efecto, si un proveedor ofrece sus servicios en la Unión —servicios de comunicación, de almacenamiento de datos, compraventas online, transacciones con criptomonedas, etc.—, los cuales se están empleando masivamente también para la comisión de hechos delictivos, ese proveedor deberá colaborar con las autoridades competentes en la Unión que se ocupan de la investigación y enjuiciamiento de los delitos. El «lugar» de almacenamiento de los datos deja de ser relevante en este sentido (23) .

Por otro lado, debe destacarse que en la versión final del Reglamento *e-evidence* se han visto corregidos algunos importantes déficits del articulado, que ya se pusieron de manifiesto durante la tramitación del instrumento.

En particular, finalmente se ha introducido el «mecanismo de notificación» a la autoridad judicial del Estado de ejecución —*vid.* art. 8 del Reglamento 2023/1543—, aunque no operará en la mayoría de los supuestos de cooperación con los proveedores de servicios.

También se ha previsto la posibilidad de que los abogados de la defensa puedan solicitar la emisión de EPOC/EPOC-PR a las autoridades competentes, conforme establezca su propio derecho nacional, en caso de que para poder articular adecuadamente su defensa necesiten datos electrónicos que almacenan los proveedores (24) .

Las limitaciones de los mecanismos tradicionales de cooperación resultan especialmente evidentes cuando se trata de obtener datos electrónicos caracterizados por su volatilidad y dispersión geográfica. Esta circunstancia ha impulsado la búsqueda de instrumentos más ágiles y eficaces

Otro aspecto que supondrá una clara ventaja respecto de la situación actual será la instauración de un canal seguro de transmisión de la información entre autoridades nacionales y proveedores de servicios. Esta cuestión es esencial para que pueda funcionar de manera rápida y segura un instrumento de cooperación de estas características.

El llamado «sistema informático descentralizado» (25) permitirá esa comunicación ágil y fiable, el intercambio de formularios y la transmisión de los datos requeridos; su uso será obligatorio para todos los implicados.

Además, ha de valorarse positivamente que, a fin de que dicho sistema no suponga un coste inasumible para las pequeñas o medianas empresas del sector, se haya previsto que la Comisión ponga a disposición de los proveedores de servicios una interfaz web gratuita: el denominado «programa informático de aplicación de referencia» les permitirá acceder sin coste al «sistema informático descentralizado».

En todo caso, hasta que no se pueda disponer efectivamente de este concreto canal seguro de comunicación, que solo entrará en funcionamiento a partir de un año desde que la Comisión adopte el sistema informático descentralizado —*vid.* art. 34 Reglamento 2023/1543—, se tendrán que utilizar los

medios alternativos de comunicación que pudieran ser adecuados y seguros, lo que implicará una diversidad de sistemas de comunicación. Esto puede ser también una debilidad del sistema de obtención transfronteriza de información electrónica.

Ha de destacarse igualmente en este apartado de ventajas del nuevo sistema que se implanta con el paquete *e-evidence* el hecho de que Irlanda se incorpore al ámbito de aplicación de este instrumento de cooperación basado en el reconocimiento mutuo, según se puede leer en el Considerando 100.º del Reglamento 2023/1543.

Conviene recordar que este Estado de la Unión no participa de la Orden Europea de Investigación, es decir, no le vincula la Directiva 2014/41/CE (LA LEY 6702/2014), lo que ya de por sí es una debilidad de dicho mecanismo de obtención transfronteriza de pruebas en materia penal, que incluye también las electrónicas.

La incorporación de Irlanda ha de valorarse de forma especialmente positiva, más si tenemos en cuenta que importantes proveedores de servicios de comunicaciones electrónicas, de almacenamiento de datos y de la sociedad de la información en sentido más amplio, tienen ya establecimiento en ciudades irlandesas (26) , lo que desde luego facilitará la puesta en marcha de este nuevo sistema de cooperación directa, que ya venían prestando de manera voluntaria los proveedores de servicios en los casos en que era posible.

Finalmente, la necesaria transposición del «paquete *e-evidence*» a los distintos ordenamientos de los Estados miembros será una oportunidad para que éstos actualicen y mejoren las respectivas regulaciones nacionales sobre obtención y valoración de las pruebas electrónicas en el proceso penal.

Además, la inminente puesta en marcha del nuevo sistema de obtención transfronteriza de información electrónica, de manera obligatoria en todos los Estados UE, ha de ser vista igualmente como una excelente oportunidad para mejorar la formación de todos los operadores jurídicos sobre las utilidades y presupuestos de aplicación de esta nueva herramienta de uso común (27) .

III. Algunas objeciones y dudas que se plantean acerca de la normativa europea sobre «*e-evidence*»

La crítica más importante vertida sobre el sistema que se implantará con la nueva regulación tiene que ver con la «privatización» de la cooperación transfronteriza y con la falta del suficiente control judicial de la legalidad y proporcionalidad de las peticiones en el Estado de ejecución.

Si bien finalmente se atendieron una parte de las objeciones formuladas al texto inicialmente propuesto por la Comisión en 2018, incorporando a la autoridad judicial del Estado de ejecución en el control en algunas concretas órdenes de producción que recibirán los proveedores de servicios, es probable que el «mecanismo de notificación» recogido en el art. 8 del Reglamento 2023/1543 no llegue a operar en la mayoría de los supuestos que se planteen en la práctica. Por tanto, el control de la legalidad, necesidad y proporcionalidad de la solicitud de datos electrónicos a los proveedores de servicio corresponderá casi exclusivamente a la autoridad de emisión —la misma que está investigando (¡!)— y en escasa medida al propio proveedor de servicios, pues este último recibirá muy poca información sobre el asunto que se investiga y, además, podemos suponer que tendrá pocos alicientes y limitados recursos personales para verificar con suficiente rigor si los cientos o miles de órdenes que van a recibir son conformes a derecho en todos sus extremos. No olvidemos que en caso de negativa a cumplir el mandato contenido en el EPOC / EPOC-PR, el proveedor de servicios se puede tener que enfrentar a importantes sanciones penales y/o económicas.

Es interesante en este punto la lectura de uno de los últimos documentos publicados poco antes de la aprobación del «paquete *e-evidence*», redactado conjuntamente por importantes «grupos de interés» pertenecientes al ámbito de los medios de comunicación, del periodismo, de la abogacía, a otras asociaciones profesionales y también a representantes de proveedores de servicios de internet (28) . En él se concluyó, entre otros extremos, que el sistema de acceso transfronterizo a datos electrónicos en causas penales, en los términos en que estaba entonces a punto de aprobarse, tras los trílogos de diciembre de 2022, ponía en claro peligro derechos fundamentales como el debido proceso —*right to a fair trial*—, las libertades de prensa y de expresión, el derecho a la privacidad —*privacy*—, y las obligaciones de secreto y confidencialidad de algunos profesionales, como periodistas, abogados o médicos. Las salvaguardas a estos colectivos están mal diseñadas en el Reglamento —destacaban sus representantes—, pues no impedirán el acceso ilegítimo a sus comunicaciones con sus clientes y

pacientes. En muchos casos los únicos que podrían frenar un uso indebido o desproporcionado de las órdenes serían los proveedores de servicios, pero sus facultades en este sentido son limitadas, e incluso desincentivadas por las amenazas de sanción.

Exponían además estos colectivos que el «mecanismo de notificación» del art. 8, tal y como ha sido finalmente recogido en el Reglamento, es insuficiente y básicamente inoperante —*trickle and toothless*—, y aunque se haya propuesto como una solución para mejorar el texto inicialmente propuesto, será en la práctica una excepción, y no la regla en el funcionamiento del sistema.

En consecuencia, el instrumento no aporta suficiente seguridad jurídica a los proveedores de servicios y se corre el riesgo de que se pueda emplear para perseguir a periodistas, defensores de los derechos humanos, opositores políticos o abogados, entre otros. Además, se concluía en el referido documento que el legislador de la Unión no había tenido suficientemente en cuenta que ciertos contextos nacionales cuentan con un Estado de Derecho —*Rule of Law*— debilitado, donde concurren riesgos claros de represión política.

Otra de las debilidades del sistema de cooperación finalmente adoptado, tras arduas negociaciones, tiene que ver precisamente con la complejidad de la normativa que lo regula, lo que también obliga a plantearse si en efecto reemplazará a la actual y mucho más sencilla «cooperación voluntaria directa».

El Reglamento 2023/1543 consta de relativamente pocos artículos —26 (29) si excluimos las disposiciones finales—, muchos Considerandos —102—, incluso demasiados si tenemos en cuenta que algunos de ellos añaden especificaciones relevantes que, a nuestro juicio, deberían estar en el articulado.

Concretamente en este instrumento es importante fijarse bien en lo que contienen o no contienen los respectivos formularios que figuran en los Anexos. Por ejemplo, en el hecho de que el formulario EPOC que recibirá el proveedor de servicios tendrá mucha menos información sobre la causa que se investiga que el formulario que se remitirá a la autoridad de ejecución cuando se le tenga que notificar la orden de producción en aplicación del art. 8.

Además, si no se concreta muy bien en el EPOC la información que se le está demandando al proveedor de servicios, esa solicitud puede ser denegada por desproporcionada, o no se recibirán los datos que realmente se necesitan, o incluso se recibirán demasiados y no se podrán procesar de manera eficaz, con la agilidad imprescindible para seguir adelante con la investigación.

Téngase en cuenta también, como han destacado los *Informes SIRIUS* ya citados, que la cooperación voluntaria directa entre autoridades nacionales y los principales proveedores de servicios de internet viene funcionando hasta ahora de manera satisfactoria en términos generales. Hemos de suponer que cuando entre en vigor el «paquete *e-evidence*», también en esos casos en que ahora es posible tal cooperación directa, se deberá pasar a emplear el sistema EPOC / EPOC-PR, lo que en cierta medida va a añadir complejidad a la obtención de ese tipo de datos que no son de contenido; por cierto, los que más se solicitan en la práctica.

Nos tenemos que preguntar entonces si quedará «abolida» la cooperación voluntaria directa con los proveedores de servicios, o si por el contrario podrán éstos seguir dando respuesta como hasta ahora a esas peticiones.

Entendemos que no, que la cooperación se tendrá que canalizar necesariamente a través del nuevo sistema que establece el paquete «*e-evidence*», y más cuando será obligatoria la implantación de un específico «sistema informático descentralizado» para la transmisión de los datos solicitados.

En cualquier caso, estimamos que este extremo tan importante debería haber quedado bien claro en la norma, pues en otro caso es posible que se mantenga la duplicidad de sistemas de obtención de información electrónica, lo que suponemos no era el deseo del legislador UE.

Otra de las objeciones que se plantean tiene que ver con la falta de concreción y de armonización de algunos de los motivos de denegación del cumplimiento del EPOC.

No están en absoluto armonizados en el ámbito de la Unión los supuestos en que los datos podrían estar «*protegidos por inmunidades o privilegios concedidos en virtud del Estado de ejecución*», o «*cubiertos por normas sobre la determinación o limitación de la responsabilidad penal relacionadas con la libertad de prensa o la libertad de expresión en otros medios de comunicación*», cuestiones a las que

se hace referencia en el art. 12 del Reglamento como motivos de denegación de la orden europea de producción.

En consecuencia, esta carencia puede afectar a la eficacia del instrumento, ya que la autoridad judicial de emisión no conocerá las normas sobre estos aspectos que operan en el Estado de ejecución, que pueden ser muy distintas de las que rigen en el Estado de emisión. Preocupa en particular la cuestión relativa a la obtención de datos de contenido que podrían afectar al «privilegio» del secreto de comunicaciones entre abogados y sus clientes.

Igualmente es un motivo muy importante de preocupación para las autoridades encargadas de la investigación que no exista en la UE un marco normativo armonizado sobre los concretos periodos mínimos de conservación de datos por parte de los proveedores de servicios con fines policiales o de investigación.

Si bien los plazos máximos de conservación de los datos por los proveedores están *en cierta medida* limitados por la normativa UE y jurisprudencia del TJUE al respecto, sigue habiendo muchas diferencias entre esos plazos de conservación de los distintos tipos de datos, por lo que cuando las autoridades nacionales solicitan datos a los proveedores en el marco de una investigación, no pueden saber de antemano si esos datos se siguen conservando, o no. Dependerá de cada uno de los proveedores de servicios a que se estén dirigiendo.

Por lo tanto, puede que se estén pidiendo datos que los proveedores ya han eliminado en cumplimiento de las respectivas normas nacionales que les vinculan o de sus propias reglas de funcionamiento interno, y entonces todo el trabajo realizado para preparar y transmitir el EPOC habrá sido en vano.

Este problema de la «*Lack of EU-Wide data retention framework for law enforcement purposes*» ha sido reiteradamente puesto de relieve por los operadores jurídicos, por las autoridades de investigación y también por los propios proveedores de servicios de internet (30) .

La eficacia del nuevo sistema dependerá de su capacidad para compatibilizar la rapidez en el acceso a la información con el respeto a las garantías procesales y a los derechos fundamentales. La práctica determinará el alcance real de ese equilibrio.

Se plantean también importantes objeciones en relación con el llamado «principio de especialidad», pues según el articulado del Reglamento 2023/1543 este principio no operará en relación con la obtención y uso de pruebas consistentes en datos almacenados por los proveedores de servicios.

De la lectura del escueto apartado 5.º del art. 18 del Reglamento hemos de deducir que sí será posible transmitir a cualesquiera otro Estado miembro las pruebas electrónicas que reciba la autoridad del Estado de emisión del EPOC, aunque no se indica en el Reglamento con qué presupuestos o condiciones. Además, puesto que se admite que es posible transferir la información recibida a las autoridades de otros Estados, habrá que suponer que también podrá emplearse en otras causas distintas que se sustancien en el mismo Estado de emisión.

Otro problema importante que se plantea ya actualmente en la práctica tiene que ver con la encriptación o cifrado de los datos que se recibirán del proveedor de servicios, ya que puede resultar que la respuesta al EPOC remitido resulte en último término ineficaz.

Indica el Considerando 20.º del Reglamento que los datos que soliciten las autoridades serán entregados por el proveedor de servicios «*con independencia de que estén cifrados o no*», y no se establece «*ninguna obligación de descifrar los datos para los prestadores de servicios*».

Por tanto, los datos se entregarán a las autoridades nacionales que han emitido el EPOC tal y como los tenga almacenados el proveedor. En muchas ocasiones el propio proveedor no tendrá las claves de desencriptación de los datos que almacena, que solo conocerá el usuario, por lo que, si éste no colabora, las respectivas autoridades nacionales expertas en la materia tendrán que tratar de acceder a la información que se necesite haciendo uso de los sistemas de descifrado o desencriptación que pudieran tener a su alcance. Lamentablemente, estos no siempre darán los resultados deseados, sobre todo si se necesita acceder a datos de contenido o a información sobre almacenamiento o intercambio de criptomonedas, por lo que en último término la eficacia de la cooperación se verá frustrada.

Se nos plantea por otro lado la duda de si los respectivos proveedores de servicios podrán cumplir con todas las solicitudes de datos que reciban de las distintas autoridades nacionales dentro de los estrictos

plazos establecidos en el Reglamento. Tendrán que dar respuesta a las órdenes de producción que reciban en un máximo de 10 días tras la recepción del EPOC, o de 8 horas en caso de urgencia.

Es previsible que los representantes o establecimientos designados por los proveedores de servicios al menos en un Estado miembro reciban cientos o miles de peticiones de datos. Algunas serán sencillas, pero otras requerirán una respuesta más compleja o incluso deberán ser rechazadas, con la correspondiente motivación.

Para que el nuevo sistema funcione globalmente, también los proveedores de servicios tendrán que asignar suficientes recursos personales y materiales que les permitan cumplir en tiempo y forma con estas obligaciones que les impone el «paquete *e-evidence*».

Estimamos también que es una amenaza severa para la eficacia del nuevo sistema que se implanta con el «paquete *e-evidence*» el uso que se pueda hacer de la llamada «*obligación de reexamen*» en los casos en que el cumplimiento de algunas órdenes pudiera entrar en conflicto con el Derecho aplicable de un tercer país. Tendremos que estar atentos a la invocación por parte de los proveedores de servicios de «*objeciones motivadas*» y, en general, a la aplicación que en el futuro se haga del «*procedimiento de reexamen*» del art. 17 del Reglamento.

Hasta que no se firme el «acuerdo ejecutivo» que se está negociando entre los Estados Unidos y la Unión Europea, y/o sea aplicable el 2.º Protocolo Adicional al Convenio de Budapest, del que también participa EE.UU., los proveedores de servicios que tienen su sede precisamente en EE.UU., muchos y muy importantes, tendrán que resolver los conflictos jurídicos que se les puedan plantear cuando reciban un EPOC, pues estarán obligados a ejecutar esas órdenes europeas de entrega de datos, pero al mismo tiempo deberán considerar la legislación del país donde se encuentra su sede, que también les vincula; en particular, en este momento, la ya referida *CLOUD Act* estadounidense.

Veremos si finalmente estas previsiones del Reglamento 2023/1543 sobre la «*obligación de reexamen*» no acaban siendo una amenaza real para la efectividad del nuevo sistema de obtención transfronteriza de información electrónica.

IV. Bibliografía

ARANGÜENA FANEGO, C.: «El reglamento e-evidence y las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales», en *Derecho Procesal y ciudadanía,* E. González Pillado (Dir.), Barcelona, 2025, pp. 377-402.

BÖSE, M., «Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?», *Kriminalpolitische Zeitschrift,* 3/2019, pp. 140-147.

BURCHARD, Ch., «Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamental prinzipien der internationalen Zusammenarbeit in Strafsachen», Teil II, *Zeitschrift für die gesamte Strafrechtswissenschaft*, 7-8/2018, pp. 249-267.

COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE —CCBE—: *Posición del CCBE sobre la Propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos del enjuiciamiento penal*, de 19 de octubre de 2018. Accesible en: https://www.abogacia.es/wp-content/uploads/2019/03/Posicionamiento-sobre-ordenes-europeas-de-entrega-y-conservacion-de-pruebas-electronicas-a-efectos-de-enjuiciamiento-penal.pdf

DE BUSSER, E., «EU-USA Digital Data Exchange to Combat Financial Crime: Fast is the New Slow», *German Law Journal*, vol. 19, Issue 5, 2018, pp. 1251-1267.

DE HOYOS SANCHO, M., *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Análisis y valoración del «e-evidence package».* Aranzadi, Madrid, 2024.

DE HOYOS SANCHO, M., «Informe Sirius 2024 sobre la prueba electrónica transfronteriza en la Unión Europea: conclusiones y propuestas», *La Ley Unión Europea*, n.º 133, febrero 2025, pp. 1-7.

ESPINA RAMOS, J., «European Preservation and Production Orders: A Non-Exclusive Approach to e-Evidence within the EU», *EUCRIM*, n.º 3/2025, pp. 216-219.

FAIR TRIALS, *Consultation Paper: E-evidence Position Paper*. Febrero 2019. Accesible en: https://www.fairtrials.org/app/uploads/2022/02/E-evidence-position-paper-February-2019.pdf, Último acceso 25.3.2025.

GIALUZ, M. y DELLA TORRE, J., «Lotta alla criminalità nel cyberspazio: la Commisione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali», *Diritto Penale Contemporaneo*, n.º 5, 2018, pp. 277-294.

MURIEL DIEGUEZ, J. A., «El Anteproyecto e-evidence. Primeras impresiones», *La Ley Unión Europea*, n.º 148, junio 2026, pp. 1 y ss.

TOSZA, S.: «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. II (2), 2020, pp. 161-183.

(1)

Este trabajo es resultado del Proyecto financiado por el Ministerio de Ciencia, Innovación y Universidades – Agencia Estatal de Investigación: *«Proceso penal y espacio de libertad, seguridad y justicia: Garantías, cooperación transfronteriza y digitalización»* —PID2023-152074NB-I00—, así como del Grupo de Investigación Reconocido «*Garantías procesales y Unión Europea*», de la Universidad de Valladolid, y del proyecto del mismo nombre de la Junta de Castilla y León —VA033G24—.

(2)

El volumen de datos electrónicos requeridos a los distintos proveedores de servicios creció un 22% en el último año computado. La tasa de éxito de las peticiones ascendió al 74%, el mejor porcentaje desde que se elaboran este tipo de estudios e informes. La mayor tasa de éxito en la entrega de datos (82%) corresponde a las peticiones cursadas a Google. Véase los últimos Informes publicados por Europol y Eurojust sobre la materia —EU Electronic Evidence Situation Report—: SIRIUS 2023 y SIRIUS 2024 «Cross-Border access to electronic evidence»: https://www.europol.europa.eu/operations-services-innovation/sirius-project, así como M. De Hoyos Sancho, «Informe Sirius 2024 sobre la prueba electrónica transfronteriza en la Unión Europea: conclusions y propuestas», *La Ley Unión Europea*, n.º 133, febrero 2025, pp.1-7.

(3)

Directiva 2014/41/CE, de 3 de abril de 2014 (LA LEY 6702/2014): https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014L0041. Aplicable en el ámbito de la Unión Europea, excepto en Irlanda y Dinamarca.

(4)

Estos inconvenientes mostraron la necesidad de superar el llamado «principio de territorialidad», clásico de la materia probatoria, pues la información requerida ya no está almacenada de forma estable en un determinado lugar, sino que se encuentra «en la nube», vinculada a un proveedor de servicio; por lo tanto, si éste opera en la UE, deberá colaborar con las autoridades encargadas de la investigación de los delitos. Véase S. Tosza, «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. II (2), 2020, pp. 161-183, esp. p. 170.

(5)

Véase el citado Informe SIRIUS 2024, pp. 22 ss.

(6)

Convenio suscrito en el marco del Consejo de Europa con fecha 23 de noviembre de 2001. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

(7)

Firmado el 25 de junio de 2003, DOUE 19.7.2003. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22003A0719(02)

(8)

Un amplio estudio sobre este próximo escenario normativo puede encontrarse en: M. De Hoyos Sancho, *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales. Análisis y valoración del «e-evidence package».* Aranzadi, Madrid, 2024.

(9)

Incluso Irlanda notificó su deseo de participar en la adopción de este Reglamento, extremo este relevante, pues este país no participa del sistema OEI. Véase Considerando 101 del Reglamento (UE) 2023/1543 (LA LEY 22209/2023).

(10)

Puede consultarse en: 2026-0618-APL-e-evidence-TAIP.pdf

(11)

Así lo adelantaba ya C. Arangüena Fanego, en su trabajo: «El reglamento e-evidence y las órdenes europeas de producción y conservación a efectos de prueba electrónica en procesos penales», en *Derecho Procesal y ciudadanía,* E. González Pillado (dir.), Barcelona, 2025, pp. 377 y ss, esp. p. 398.

(12)

Véase a este respecto el reciente trabajo de Muriel Dieguez, J. A.: «El Anteproyecto *e-evidence*. Primeras impresiones», publicado en esta misma revista *La Ley Unión Europea*, en su n.º 148, junio 2026.

(13)

European Production Order Certificate.

(14)

European Preservation Order Certificate. Órdenes de conservación que lógicamente también podrán emitir los órganos jurisdiccionales y fiscales competentes en el procedimiento en curso.

(15)

Si no se concediera la validación posterior, la policía debería retirar la orden inmediatamente, suprimiendo o restringiendo el uso de los datos previamente obtenidos.

(16)

Como puede leerse en el propio Anteproyecto, Véase p. 5, se configura un régimen sancionador excepcional, tal y como prevé el Reglamento 2023/1543, al atribuir a los jueces la imposición de sanciones de naturaleza administrativa.

(17)

Era necesario por tanto articular ese «*fast-track-line*» al que ya se refiriera De Busser, «EU-USA Digital Data Exchange to Combat Financial Crime: Fast is the New Slow», *German Law Journal*, vol. 19, n.º 5, 2018, pp. 1251-1267, esp. p. 1266.

(18)

No obstante, algunos autores, como Burchard, Ch.: «Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamental prinzipien der internationalen Zusammenarbeit in Strafsachen», Teil II, *Zeitschrift für die gesamte Strafrechtswissenschaft*, 7-8/2018, pp. 249-267, esp. pp. 253 y ss. o Böse, M. «Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel –Rückzug des Staates aus der Rechtshilfe?», *Kriminalpolitische Zeitschrift,* 3/2019, pp. 140-147, esp. p. 146, proponían mejorar/reforzar la OEI y tratar de superar sus posibles inconvenientes, en vez de poner en marcha un nuevo instrumento que prescindiera del principio de territorialidad en la materia y propugnara como solución la privatización de la cooperación transfronteriza.

(19)

Algunos Estados miembros han ampliado ya unilateralmente sus respectivas facultades de actuación, aprobando legislación nacional que les permite emitir órdenes de entrega de datos a proveedores de servicios que operan en su concreto territorio, aunque los datos estén almacenados en el extranjero; así lo han hecho ya, *v.gr.,* Alemania y Bélgica. Véase Burchard, Ch.: «Der grenzüberschreitende Zugriff…», *op. cit.,* Parte I, p. 191. Esto plantea inconvenientes de distinta índole, pues cuando esas medidas son adoptadas a título individual por cada uno de los Estados, conllevan *de facto* obstáculos a la libre prestación de servicios en el mercado interior, por lo que es claramente preferible una acción normativa «a escala de la Unión», que obligue por igual a todos los proveedores de servicios que ofrecen sus servicios en cualquier Estado/s de la Unión.

(20)

Algunos proveedores de servicios han creado portales en línea dedicados específicamente a prestar esa colaboración a las autoridades competentes, por ejemplo: Airbnb, Google, Microsoft, Meta, Uber, Twitter, WhatsApp o Zoom. Permiten conocer el estado de la solicitud, descargar las respuestas de forma segura y agilizar la comunicación entre autoridades y proveedores. Véase El citado Informe SIRIUS 2023, pp. 21 y 24.

(21)

Clarifying Lawful Overseas Use of Data Act —CLOUD Act—: H. R. 4943, de 2.6.2018. Accesible en: https://www.congress.gov/bill/115th-congress/house-bill/4943/text

(22)

Ya apuntaron en su día Gialuz y Della Torre que el uso del instrumento Reglamento era buena prueba de que las instituciones UE se fiaban realmente poco de cómo los Estados miembros recibían los instrumentos euro-unitarios en materia procesal penal, por lo que en este caso habían optado por eludir el problema, proponiendo un acto *self-executing*. Véase su trabajo «Lotta alla criminalità nel cyberspazio: la Commisione presenta due

proposte per facilitare la circolazione delle prove elettroniche nei processi penali», *Diritto Penale Contemporaneo*, n.º 5, 2018, pp. 277-294, esp. p. 292.

(23)

Esta conclusión o valoración positiva sobre el apartamiento del principio de territorialidad no es unánime entre la doctrina que se ha ocupado del estudio del tema. Así, destacadamente Burchard considera que se debería haber mantenido la vigencia de este principio rector, pues la «privatización» de la cooperación transfronteriza no es la mejor solución normativa a este problema. Véase «Der grenzüberschreitende Zugriff…», *op. cit.*, pp. 249 y ss.

(24)

En este punto fueron determinantes los contundentes informes emitidos por la Abogacía europea —*Council of Bars and Law Societies of Europe*— y por FAIR TRIALS, reclamando insistentemente esta posibilidad que es esencial para ejercer una defensa con igualdad de armas.

(25)

Véase Considerando 21.º: «Red de sistemas informáticos y puntos de acceso interoperables que opera bajo la responsabilidad y la gestión individuales de cada Estado miembro, agencia u organismo de la Unión, y permite que el intercambio transfronterizo de información tenga lugar de modo seguro y fiable». Véase también arts. 19 y ss. del Reglamento 2023/1543.

(26)

Así, por ejemplo, en Dublín está la sede europea de Google y en particular su «centro de datos»; la sede europea de Apple está en Cork, también en Irlanda.

(27)

Destaca la importancia de la correcta formación y de un cierto cambio/apertura de mentalidad de todos los operadores jurídicos en la aplicación de esta nueva normativa, precisamente por las peculiaridades del instrumento, Espina Ramos, J.: «European Preservation and Production Orders: A Non-Exclusive Approach to e-evidence within the EU», *EUCRIM*, n.º 3/2025, pp. 216 y ss., esp. p. 219.

(28)

Documento conjunto publicado en Bruselas el 12 de junio de 2023, suscrito por importantes colectivos profesionales directamente interesados en la materia, entre otros: Committee to Protect Journalists (CPJ), Council of Bars and Law Societies of Europe (CCBE), Association of the Internet Industry, European Digital Rights (EDRi), European Federation of Journalists (EFJ): *Plenary vote on the «e-evidence package»Regulation and Directive on «European production and preservation orders for electronic evidence in criminal matters» and «legal representatives»*

https://www.cpme.eu/api/documents/adopted/2023/06/Joint-Letter-Plenary-Vote-E-evidence-13-June-2023.pdf

(29)

Aunque algunos de ellos abarcan más de tres páginas del D.O.U.E.

(30)

Véase Informe SIRIUS 2023, *supra cit.,* esp. pp. 8, 9, 55 y 63.