

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.

SUMARIO 1.Introducción. 2.El Reglamento 2023/1543. Antecedentes. El principio de primacía del Derecho de la Unión Europea y de reconocimiento mutuo. La privatización de la cooperación jurídica internacional. Las órdenes europeas de producción y conservación de pruebas. 3. La autoridad competente para emitir una orden al amparo del Reglamento 2023/1543. 4. Las condiciones para emitir la orden. 5. Notificación a la autoridad de ejecución. 6. La ejecución de la orden europea de producción y de ejecución. 7. Motivos de denegación. 8. Sanciones. 9. Derechos de la persona cuyos datos se solicitan. 10. Conflicto de leyes. 11. La designación de establecimientos y representantes legales para recabar las pruebas electrónicas. 12. El sistema descentralizado europeo. 13. Conclusiones.

1. Introduccion.

La obtención y preservación de pruebas electrónicas se ha convertido en uno de los mayores desafíos para el derecho penal. La digitalización de la vida social y económica ha generado un volumen creciente de datos cuya volatilidad, dispersión geográfica y dependencia de proveedores privados exige mecanismos de cooperación internacional más ágiles y eficaces. En este contexto, el Reglamento (UE) 2023/1543 representa un punto de inflexión al introducir un modelo de cooperación directa entre autoridades judiciales y prestadores de servicios, superando las limitaciones de los instrumentos tradicionales como las comisiones rogatorias o incluso la Orden Europea de Investigación.

El análisis del Reglamento permite comprender no solo su estructura y funcionamiento, sino también las tensiones que genera: desde el debate sobre la “privatización” de la cooperación jurídica hasta los riesgos derivados de trasladar a empresas tecnológicas funciones de control que antes correspondían exclusivamente a autoridades públicas. Al mismo tiempo, el Reglamento se inserta en un ecosistema normativo más amplio que condiciona su aplicación práctica y revela la complejidad del acceso transfronterizo a la evidencia digital.

2. El Reglamento 1543/2023. Antecedentes. El principio de primacía del Derecho de la Unión Europea y de reconocimiento mutuo. La privatización de la cooperación jurídica internacional. Las órdenes europeas de producción y conservación de pruebas.

La transformación digital de la sociedad ha modificado de forma profunda tanto la comisión de delitos como su investigación. Gran parte de la actividad humana se desarrolla hoy en el ámbito digital. Comunicaciones, transacciones económicas, accesos a sistemas, interacciones en redes sociales o almacenamiento de documentos tienen lugar en entornos tecnológicos que generan datos susceptibles de ser utilizados en procedimientos penales como instrumentos de investigación o elementos de prueba.

La obtención de estos datos plantea, sin embargo, dificultades específicas. A diferencia de la evidencia física, los datos electrónicos son fácilmente alterables y, en muchos casos, volátiles. Ello puede deberse tanto a la inexistencia de obligaciones legales de conservación como a la aplicación de políticas de eliminación de datos por parte de los proveedores de servicios, frecuentemente vinculadas a la protección de datos personales. A estas dificultades se añade la relativa a la localización de la información. El uso generalizado de servicios en la nube y de infraestructuras tecnológicas distribuidas implica que datos relevantes para una investigación iniciada en un Estado puedan encontrarse almacenados en servidores situados en otros países y gestionados por empresas multinacionales sometidas a diferentes ordenamientos jurídicos (1) ¹.

Esta dimensión transnacional del entorno digital genera un problema estructural para el proceso penal. Mientras que la comisión del delito puede producirse de forma inmediata y sin atender a fronteras, la respuesta penal sigue dependiendo en gran medida de mecanismos de cooperación judicial entre Estados. La dispersión geográfica de los datos, la diversidad normativa y la necesidad de respetar los derechos fundamentales complican el acceso rápido y legítimo a la información.

Tradicionalmente, la asistencia judicial internacional se ha articulado mediante comisiones rogatorias. Sin embargo, estos instrumentos fueron concebidos para una criminalidad esencialmente territorial. En el contexto digital, donde la rapidez resulta esencial para evitar la pérdida de información, estos procedimientos pueden resultar excesivamente lentos y poco adaptados a la realidad tecnológica actual.

Por ello, la cooperación jurídica internacional en materia penal se ha convertido en una exigencia imprescindible. No basta con que los Estados colaboren; es necesario que lo hagan de forma ágil, coordinada y sobre la base de la confianza mutua. La eficacia de la investigación penal depende en gran medida de que las autoridades puedan activar

¹ Delgado Martín, J. Prueba digital internacional. El Reglamento E-Evidence. *Revista La Ley, Sección Ciberderecho*, 15 de septiembre de 2023, nº76.

mecanismos de conservación inmediata de datos y acceder a ellos en plazos compatibles con su volatilidad.

Al mismo tiempo, esta agilización no puede lograrse a costa de debilitar las garantías procesales. La obtención transfronteriza de prueba electrónica debe conciliar la eficacia investigadora con el respeto a los derechos fundamentales, en particular el derecho a la intimidad y a un proceso con todas las garantías. El desafío consiste, por tanto, en diseñar instrumentos que permitan superar los obstáculos derivados de las fronteras sin generar espacios de desprotección jurídica.

Actualmente, la cooperación jurídica internacional para la obtención de prueba electrónica se articula a través de diversos instrumentos, entre los que destacan las comisiones rogatorias, la entrega voluntaria de información por parte de los proveedores de servicios conforme a sus políticas internas, la Orden Europea de Investigación y, más recientemente, las órdenes europeas de producción y conservación de pruebas electrónicas introducidas por el Reglamento (UE) 2023/1543.

Antes del desarrollo de estos instrumentos el principal marco internacional de cooperación en materia de ciberdelincuencia y obtención de prueba electrónica fue el Convenio del Consejo de Europa sobre la Ciberdelincuencia de 23 de noviembre de 2001, complementado posteriormente por el Protocolo Adicional de 28 de enero de 2003 y por el Segundo Protocolo Adicional de 12 de mayo de 2022 (2) ².

El Convenio de Budapest, que entró en vigor el 1 de julio de 2004, constituye el primer tratado internacional destinado específicamente a abordar los retos que plantea la criminalidad en entornos digitales. Su objetivo fundamental es doble: por un lado, promover la armonización de las legislaciones penales en materia de ciberdelincuencia y, por otro, establecer mecanismos de cooperación internacional adaptados a la naturaleza transnacional de los delitos cometidos mediante sistemas informáticos.

En este sentido, el Convenio introduce instrumentos que han resultado particularmente relevantes para la investigación penal en el entorno digital. Entre ellos destacan los mecanismos de conservación rápida de datos informáticos, destinados a evitar su pérdida antes de que pueda formalizarse una solicitud de asistencia judicial; la cooperación para la obtención en tiempo real de datos de tráfico y, en determinados casos, del contenido de las comunicaciones; o la creación de una red permanente de puntos de contacto disponibles las veinticuatro horas del día, los siete días de la semana (red 24/7), destinada a facilitar la asistencia inmediata entre las autoridades de los Estados parte.

El Convenio parte del principio de cooperación en la mayor medida posible entre las partes, estableciendo obligaciones de asistencia mutua en las investigaciones o procedimientos relacionados con sistemas y datos informáticos o dirigidos a la obtención de prueba electrónica. Asimismo, prevé la posibilidad de que un Estado transmita información a otro de forma espontánea cuando considere que puede contribuir a iniciar o desarrollar una investigación penal. Tiene la virtualidad de que al Convenio le ha seguido la creación del Comité de la Convención sobre Ciberdelincuencia (T-CY), la Oficina del

²El Convenio sobre la Ciberdelincuencia: <https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html>

Programa de Ciberdelincuencia del Consejo de Europa (C-PROC) y la *Conferencia Octopus* (3)³.

El sistema convencional se completa con reglas relativas a las condiciones de utilización de la información transmitida, a los motivos de denegación de la cooperación y a los mecanismos de comunicación entre autoridades. Con ello se pretende facilitar la cooperación internacional sin dejar de preservar los principios básicos de soberanía estatal y de protección de los derechos fundamentales.

Posteriormente, el Protocolo Adicional de 28 de enero de 2003 amplió el alcance del Convenio mediante la tipificación penal de determinados actos de carácter racista y xenófobo cometidos a través de sistemas informáticos.

Más recientemente, el Segundo Protocolo Adicional de 12 de mayo de 2022, relativo a la cooperación reforzada y a la revelación de pruebas electrónicas, introdujo mecanismos destinados a facilitar el acceso transfronterizo a determinados datos. Entre otras novedades, prevé la posibilidad de dirigir solicitudes directamente a proveedores de servicios en determinadas circunstancias, refuerza los mecanismos de cooperación entre Estados para la obtención de datos de abonado o de tráfico y establece procedimientos específicos para situaciones de emergencia en las que exista un riesgo inminente para la vida o la seguridad de las personas.

Sin embargo, este instrumento aún no ha entrado en vigor al no haberse alcanzado el número mínimo de ratificaciones exigido. Esta circunstancia pone de relieve, en cierta medida, las dificultades que presenta la adaptación de los mecanismos tradicionales de cooperación internacional a las necesidades derivadas de la investigación penal en el entorno digital, donde la rapidez en el acceso a los datos resulta con frecuencia determinante para la eficacia de la investigación.

En el ámbito europeo ha existido una evolución progresiva de los instrumentos de cooperación judicial en materia penal. Entre los antecedentes más relevantes se encuentran el Convenio Europeo de Asistencia Judicial en Materia Penal de 1959, así como su Protocolo Adicional de 17 de marzo 1978.

A este marco se sumaron posteriormente las disposiciones sobre asistencia judicial en materia penal contenidas en el Convenio de Aplicación del Acuerdo de Schengen de 1990⁴.

En una fase más reciente de integración europea, la cooperación judicial se vio reforzada con la Directiva 2014/41/UE sobre la Orden Europea de Investigación, que introdujo un instrumento más ágil para la obtención de pruebas dentro de la Unión. La Orden Europea de Investigación se basa en el principio de reconocimiento mutuo y establece un marco único para la obtención de prueba transfronteriza, obligando a los Estados a reconocer y ejecutar la orden como si se tratara de una medida de investigación adoptada por una

³ ESTÉVEZ BENITO R. La conservación y acceso a las evidencias digitales más allá de la Unión Europea. El Convenio de Budapest y sus dos Protocolos Adicionales. *Diario La Ley, Sección Ciberderecho*, nº103, 23 de febrero de 2026.

⁴La orden europea de investigación, asistencia judicial mutua y equipos conjuntos de investigación: https://e-justice.europa.eu/topics/court-procedures/criminal-cases/judicial_cooperation/european-investigation-order-mutual-legal-assistance-and-joint-investigation-teams_es

autoridad nacional, permitiendo realizar diligencias de investigación en otro Estado miembro como acceder a pruebas que ya existen.

Asimismo, en el ámbito digital también pueden encontrarse antecedentes en otras normas europeas. En particular, el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos) introdujo la figura del representante legal en la Unión para prestadores de servicios no establecidos en territorio europeo, que traten datos personales de quienes residen en la Unión Europea, anticipando soluciones jurídicas destinadas a facilitar la interacción entre autoridades europeas y operadores digitales.

En este contexto, la Unión Europea optó por avanzar en la creación de instrumentos propios destinados a facilitar el acceso transfronterizo a la prueba electrónica dentro del espacio de libertad, seguridad y justicia,

Esta evolución normativa se materializa con el Reglamento (UE) 2023/1543 que responde a las nuevas necesidades derivadas de la obtención de pruebas electrónicas en investigaciones penales. La naturaleza transnacional de los servicios digitales, frecuentemente prestados por proveedores ubicados en distintos Estados o incluso fuera de la Unión, ha puesto en cuestión el principio clásico de territorialidad que tradicionalmente ha caracterizado la cooperación jurídica internacional. Frente a ello, el nuevo marco normativo impulsa un modelo basado en un principio de funcionalidad, que permite a las autoridades judiciales dirigirse directamente a los prestadores de servicios que presten servicios en la Unión, con independencia de si están establecidos en la Unión, con independencia de la ubicación de los datos, para obtener o preservar pruebas electrónicas, reforzando así la eficacia y rapidez de las investigaciones en el espacio europeo de justicia⁵

Las órdenes europeas de producción y conservación de pruebas electrónicas en materia penal, configuran un modelo de cooperación más directo entre autoridades y proveedores de servicios y orientado a responder con mayor eficacia a la naturaleza transnacional y volátil de la evidencia digital; si bien su regulación plantea cuestiones sobre el principio de reconocimiento mutuo y la primacía del derecho de la UE, de acuerdo con la redacción de su artículo 32 que dispone que *“el presente Reglamento no afecta a otros instrumentos jurídicos, acuerdos y pactos de la Unión e internacionales relativos a la obtención de pruebas que entre en el ámbito de aplicación del presente Reglamento”*, especialmente si en la práctica se traduce en la posibilidad de que las autoridades recurran a vías alternativas potencialmente más rápidas o menos garantistas, como los mecanismos policiales previstos en el artículo 35 del Convenio de Budapest, eludiendo los cauces judiciales del Reglamento (4) ⁶.

El Reglamento 2023/1543 dispone las normas por las que una autoridad de un Estado miembro puede emitir una orden europea de conservación o de producción de pruebas a un prestador de servicios que ofrezca servicios en la Unión y esté establecido o representado por un representante legal en otro Estado miembro.

⁵ MURIEL DIÉGUEZ J.A. Implicaciones del Reglamento (UE) sobre órdenes europeas de entrega y conservación de pruebas electrónicas y la Directiva (UE) 2023/1544 en el proceso penal. *Revista Electrónica de Direito. Universidade Do Porto*, octubre de 2024, nº 3.

⁶ ESPINA RAMOS J. A. *European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU. Implications of the Union Legislator's Choice to Derogate from the Precedence of Union Law in the E-Evidence Regulation*. *Eucrim*. 2025, Vol. 20(3).

Las órdenes europeas de conservación o de producción pueden emitirse en el marco y a los efectos de un proceso penal y para fines de ejecución, en este caso con una limitación que responde al principio de proporcionalidad, ya que tienen que ser penas privativas de libertad o medidas de seguridad privativas de libertad de al menos cuatro meses; añadiendo una segunda limitación para evitar reticencias debido a la disparidad normativa en materia de enjuiciamiento en ausencia; siempre que la resolución judicial que se pretenda ejecutar no se haya dictado en rebeldía, cuando persona condenada haya huido de la justicia.

En la orden europea de producción (OEP) se ordena la entrega de pruebas electrónicas. En la orden europea de conservación (OEC) se ordena la conservación de pruebas electrónicas a los efectos de una solicitud posterior de entrega. La orden europea de conservación está pensada para preservar datos que posteriormente se quieren obtener con una orden europea de investigación o de producción.

Lo más relevante del sistema de cooperación que introduce el Reglamento es la facultad que se otorga a la autoridad del Estado miembro de comunicarse directamente con el prestador de servicios, sin tener que acudir a las autoridades del Estado miembro donde se encuentra establecido dicho prestador de servicios, como ocurre con las órdenes europeas de investigación (OEI) o las comisiones rogatorias, simplificando el procedimiento y agilizando la obtención de la información requerida.

Sin embargo, la virtud del Reglamento no está exenta de críticas, existiendo una corriente que ve la comunicación directa entre el Estado y el ente privado de prestación de servicios como una privatización de la cooperación jurídica internacional, en la medida en que los prestadores de servicios pasan a ocupar una posición central en la ejecución de las órdenes de obtención o conservación de datos, lo que supone una transformación relevante respecto del modelo tradicional de cooperación entre Estados.

Como decíamos, el nuevo esquema establece una relación directa entre las autoridades encargadas de la aplicación de la ley y los proveedores de servicios, que pasan a actuar como intermediarios obligados en la ejecución de las órdenes. Desde esta perspectiva, empresas privadas, se convierten en brazos ejecutores de las autoridades públicas. Ello ha llevado a algunos autores a hablar de una “*privatización de la confianza mutua*”, en la medida en que el sistema reduce el protagonismo de las autoridades del Estado de ejecución, que tradicionalmente ejercían un control de legalidad y de respeto de los derechos fundamentales sobre las solicitudes procedentes de otros Estados miembros. A ello se suma que estas decisiones deben adoptarse en plazos muy breves y bajo la amenaza de sanciones económicas e incluso penales en caso de incumplimiento. En tales condiciones, existe el riesgo de que los proveedores opten por ejecutar las órdenes de forma prácticamente automática para evitar responsabilidades, lo que podría debilitar el tradicional doble control de legalidad ejercido por las autoridades judiciales de los Estados implicados. Algunos autores han descrito esta transformación como un auténtico cambio de paradigma en la cooperación judicial penal ⁷.

Es cierto que con el nuevo sistema, el prestador de servicios pasa a tener la responsabilidad de controlar la legalidad o respeto de derechos fundamentales de la orden que debe ejecutar y que esas funciones exceden de sus objetivos empresariales sin

⁷ DE HOYOS SANCHO, M. *REVISTA DE ESTUDIOS EUROPEOS*, Universidad de Valladolid, 2023, n.º Extraordinario monográfico 1

embargo no debe olvidarse que el Reglamento también prevé importantes mecanismos de control.

En particular, cuando las órdenes tienen por objeto la obtención de datos de tráfico o de contenido, las categorías más invasivas, se establece la obligación de notificar la orden al Estado de ejecución. Esta notificación permite a las autoridades de dicho Estado intervenir y, en su caso, ejercer un control sobre la medida adoptada por la autoridad de emisión.

También el destinatario puede hacer intervenir a la autoridad del Estado de ejecución por ejemplo cuando considere que la ejecución de la orden europea de conservación o de producción pueda interferir en inmunidades o privilegios, o con las normas sobre determinación o limitación de la responsabilidad penal relacionadas con la libertad de prensa o la libertad de expresión en otros medios de comunicación en virtud del Derecho del Estado de ejecución. De este modo, aunque el proveedor de servicios sea el destinatario directo de la orden, el sistema conserva espacios de supervisión pública que atenúan el riesgo de un control puramente privado. En cualquier caso se echa en falta una regulación más uniforme y simplificada de los supuestos en los que la autoridad de ejecución debe intervenir, ya que la normativa actual combina excepciones, criterios de notificación, supuestos de comunicación indirecta, que puede generar inseguridad jurídica y problemas de practicidad.

Por otra parte, el protagonismo de los proveedores de servicios responde también a una necesidad estructural derivada de la naturaleza de la prueba electrónica. En este contexto, el proveedor de servicios se convierte en el único actor que puede facilitar de forma rápida y efectiva el acceso a la información necesaria para la investigación penal.

Este modelo presenta además una ventaja adicional al establecer obligaciones directas para los proveedores de servicios que operan en el mercado europeo, garantizando que estas empresas queden sometidas al Derecho de la Unión y a sus estándares de protección de derechos fundamentales. De lo contrario, las autoridades europeas se verían obligadas a depender de las políticas internas de las empresas como Google o Microsoft en materia de suministro de datos o de su disposición voluntaria a cooperar. Asimismo, el acceso a la información podría quedar condicionado a las políticas de cooperación de terceros Estados y a su normativa en esta materia.

Con la misma finalidad se aprobó en EEUU el CLOUD Act, por el que las autoridades estadounidenses pueden requerir el suministro de datos a prestadores de servicios que operen en EEUU con independencia de la ubicación de esos datos y que permite celebrar acuerdos ejecutivos con gobiernos extranjeros como el suscrito entre EEUU y el Reino Unido (2019) o Australia (2021) para facilitar la entrega directa de información, incluso de comunicaciones en tiempo real. Estos acuerdos incluyen salvaguardias sobre necesidad, proporcionalidad y revisión judicial, y establecen limitaciones para proteger a ciudadanos de EE. UU, así las órdenes no pueden afectar a personas estadounidenses o a no estadounidenses localizadas en EEUU para obtener información sobre ciudadanos estadounidenses.

Y si bien el Cloud Act supone retos para la UE por posibles desafíos de compatibilidad con el Reglamento 2023/1543 y la normativa europea de protección de datos, ello debe reforzar

la necesidad de establecer mecanismos de cooperación claros y recíprocos con EE. UU y otros socios internacionales⁸.

Y es que, este tipo de instrumentos, más que suponer una privatización de la cooperación jurídica internacional, deben entenderse como una reconfiguración de la cooperación judicial penal adaptada a las características del entorno digital.

3. La autoridad competente para emitir una orden al amparo del Reglamento 2023/1543.

El Reglamento tiene en cuenta si estamos ante una orden europea de producción o de conservación para determinar la autoridad competente para su emisión. La determinación de la autoridad competente se encuentra regulada en el artículo 4 del Reglamento.

La competencia en función de si estamos ante una orden de conservación o de producción es fruto del intenso debate que existió tras la publicación de la Propuesta inicial del Reglamento. Diversos organismos europeos como el Comité Económico Social Europeo, el Supervisor Europeo de la Protección de Datos o el Centro de Estudios Europeos advirtieron de la necesidad de que las órdenes que implicaran una mayor injerencia en la privacidad fueran controladas por una autoridad judicial independiente⁹.

En el caso de la orden europea de producción si la finalidad es obtener datos de los abonados o para obtener datos con el único fin de identificación del usuario, esto es la dirección IP, los puertos de origen y el sello de tiempo pertinentes, la fecha, hora o equivalentes técnicos de dichos identificadores e información conexas con el único fin de identificar al usuario en una investigación penal específica; la autoridad competente será el juez, tribunal, juez de instrucción o fiscal competente en el asunto de que se trate. El Reglamento dispone que también podrá emitirla cualquier autoridad que de acuerdo con la legislación del Estado emisor actúe como autoridad de investigación en el proceso penal y tenga competencia para obtener pruebas, siempre que la orden sea previamente validada por un juez, tribunal o juez de instrucción del Estado emisor.

Si lo que se pretende obtener son datos de tráfico o de contenido se excluye como autoridad competente al fiscal.

Los datos de tráfico se definen como los metadatos generados o tratados por un prestador de servicios digitales que describen cómo se transmite o utiliza un servicio, incluyendo información técnica como el origen y destino de una comunicación, la fecha y hora, la duración, la ubicación del dispositivo, el tamaño, la ruta, el protocolo usado y los datos sobre el inicio y fin de una sesión de acceso, la fecha, la hora de acceso, la conexión al servicio o la desconexión.

Los datos de contenido son los datos en formato digital que no son de tráfico ni de abonados.

⁸ The Cloud Act: <https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf>

⁹ CUADRADO SALINAS, C. La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?. *IUS ET SCIENTIA*, 2023, Vol.9 nº2.

En el caso de las órdenes europeas de conservación es competente el juez, tribunal, juez de instrucción o fiscal que tenga la competencia en el asunto de que se trate. El Reglamento dispone que también podrá emitirla cualquier autoridad que de acuerdo con la legislación del Estado emisor actúe como autoridad de investigación en el proceso penal y tenga competencia para obtener pruebas, siempre que la orden sea previamente validada por un juez, tribunal o juez de instrucción del Estado emisor.

La actual regulación puede llevar a la paradójica situación en que el fiscal que ha sido competente para emitir una orden europea de conservación no sea posteriormente competente para emitir la orden europea de producción de los datos que se han conservado¹⁰.

En casos urgentes, cuando se trate de órdenes de conservación o de producción para obtener datos de abonados o datos solicitados con el fin de identificar al usuario, las autoridades no judiciales competentes no necesitarán de la validación judicial previa cuando esta no pueda obtenerse a tiempo siempre que de acuerdo con la legislación nacional puedan emitir órdenes en un asunto nacional similar sin validación previa. En estos casos la validación se obtendrá ex post, debiendo solicitarse en el plazo máximo de 48 horas; si no se concede, la orden se anula y los datos que hayan podido obtenerse deberán eliminarse.

Por situación de urgencia debe entenderse aquella situación en la que existe un riesgo inminente para la vida, la integridad física o la seguridad de una persona o infraestructura esencial cuya perturbación o destrucción suponga una amenaza inmediata para las personas, ya sea directamente o porque cause graves perjuicios al suministro de bienes básicos para la población o al funcionamiento esencial del Estado.

4. Las condiciones para emitir la orden.

El Reglamento también regula de forma distinta las condiciones que deben concurrir para emitir una orden europea de conservación o de producción en función de su contenido. Ahora bien, la orden debe ser necesaria y proporcionada teniendo en cuenta los derechos de la persona sospechosa o acusada, y solo podrá emitirse si pudiese haberse emitido una orden similar en las mismas condiciones en un asunto nacional similar.

Si la orden europea de producción tiene por objeto obtener datos de los abonados o datos solicitados con el fin de identificar al usuario, se puede emitir la orden para todas las infracciones penales y fines de ejecución de una pena o medida de seguridad privativas de libertad de al menos cuatro meses, tras un proceso penal, impuestas por una resolución que no se haya dictado en rebeldía en los casos en que la persona condenada haya huido de la justicia.

Si se pretenden obtener datos de tráfico o de contenido, la emisión se condiciona a un requisito de proporcionalidad o de especialidad: la infracción penal tiene que estar castigada en el Estado emisor con una pena máxima privativa de libertad de al menos tres años. También se admite la orden de producción para obtener datos de tráfico o de contenido cuando se trate de infracciones penales definidas en los artículos 3 a 12 y 14 de

¹⁰ GÓMEZ AMIGO L. Estudio de las órdenes europeas de producción y conservación: un instrumento para la obtención transfronteriza de pruebas penales electrónicas. *Revista Española de Derecho Europeo*, octubre-diciembre de 2024, n° 92.

la Directiva 2017/541, relativa a la lucha contra el terrorismo o cuando se trate de infracciones penales cometidas total o parcialmente por medio de un sistema de información, siempre que sean delitos de los definidos en los artículos 3 a 8 de la Directiva 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, en los artículos 3 a 7 de la Directiva 2011/93, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil; y en los artículos 3 a 8 de la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información.

Por último, procede con fines de ejecución de penas o medidas de seguridad privativas de libertad de al menos cuatro meses tras un proceso penal impuestas por una resolución que no se haya dictado en rebeldía en los casos en que la persona condenada haya huido, por infracciones penales de las indicadas anteriormente (infracciones castigadas con pena máxima privativa de libertad de al menos tres años, delitos de terrorismo o delitos cometidos con sistemas de información de los ya referidos)

Especialmente interesantes son las previsiones que hace el artículo 5 del Reglamento en los apartados 8, 9 y 10 para solventar situaciones problemáticas que pudieran afectar a su eficacia.

En primer lugar, cuando los datos se almacenan o tratan en infraestructuras proporcionadas por un prestador de servicios a una autoridad pública, solo puede emitirse la orden si dicha autoridad se encuentra en el Estado que la emite. Es decir, las autoridades de un Estado no pueden emitir una orden europea de producción y dirigirse directamente contra el prestador de servicios que almacena los datos de las autoridades públicas de otro Estado. Admitir lo contrario podría suponer un ataque contra la soberanía y la seguridad nacional, convirtiendo el Reglamento en un atajo para obtener información de otro Estado sin las debidas garantías.

En segundo lugar, cuando los datos están protegidos por secreto profesional, únicamente pueden solicitarse datos de tráfico (salvo los destinados a identificar al usuario) o datos de contenido, en circunstancias específicas: a) cuando el profesional resida en el Estado emisor, b) cuando contactarlo perjudique la investigación o c) cuando el profesional haya renunciado al secreto profesional.

Finalmente, si existe la sospecha de que los datos están protegidos por inmunidades, privilegios o normas relacionadas con la libertad de prensa en el Estado de ejecución, la autoridad emisora debe solicitar aclaraciones también mediante consulta a las autoridades competentes del Estado de ejecución, bien directamente o bien a través de Eurojust o de la Red Judicial Europea y, si confirma dicha protección, no puede emitir la orden.

En el caso de las órdenes europeas de conservación serán necesarias y proporcionadas a efectos de impedir la retirada, supresión o alteración de datos con vistas a emitir una solicitud posterior de entrega de estos datos a través de la asistencia judicial mutua, una orden europea de investigación o una orden europea de producción, teniendo en cuenta los derechos de la persona sospechosa o acusada.

Se pueden emitir para todas las infracciones penales si pudieran emitirse en las mismas condiciones en un asunto nacional similar y para fines de ejecución de una pena o medida de seguridad privativa de libertad de al menos cuatro meses.

5. Notificación a la autoridad de ejecución.

Como venimos explicando, el Reglamento establece un sistema de comunicación directa entre el Estado y el prestador de servicios establecido en otro Estado miembro. Al objeto de dotar de mayores garantías al procedimiento y reforzar la protección de los derechos fundamentales que pueden verse afectados en el artículo 8 del Reglamento se prevé la notificación de la emisión de la orden a la autoridad del Estado de ejecución.

Sin embargo el legislador vuelve a distinguir y reserva la notificación para las órdenes europeas de producción de datos de tráfico, excepto los datos solicitados con el único fin de identificar al usuario; o de contenido, es decir, en los dos supuestos más invasivos, la autoridad emisora además de la comunicación que tenga con el prestador de servicios, debe notificar la orden a la autoridad de ejecución, evitando que el control de legalidad recaiga en manos exclusivamente del prestador de servicios.

La notificación no se configura como un mero trámite formal sino que tiene un efecto suspensivo salvo razones de urgencia en las obligaciones del destinatario de la orden.

Se prevén dos supuestos en los que no es necesaria la notificación:

-si las personas cuyos datos se solicitan viven en el Estado emisor. En este caso se entiende que la persona cuyos datos van a obtenerse no precisa de la protección del Estado de ejecución.

-si la infracción se comete, se está cometiendo o es probable que se cometa en el Estado emisor. En este caso se entiende que en nada se ven comprometidas la competencia, jurisdicción o intereses del Estado de ejecución.

En la propuesta legislativa que realiza la Fiscalía de acuerdo con la Memoria elevada al Gobierno en 2024, se propone en el Acuerdo de Adaptación del 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 ejecución de penas privativas de libertad a raíz de procesos penales que la autoridad de ejecución en España sea el Ministerio Fiscal, tomando de precedente la intervención del Ministerio Fiscal en las órdenes europeas de investigación. Se propone así mismo que la Unidad de Cooperación Internacional de la Fiscalía (UCIF) asuma la recepción centralizada de las órdenes, gestionándolas mediante el sistema CRIS/CJI y distribuyéndolas entre los delegados competentes¹¹.

6. La ejecución de la orden europea de producción y de ejecución.

Las órdenes europeas de producción y de conservación se dirigen directamente desde la autoridad emisora al establecimiento designado o al representante legal del prestador de servicios.

1. Orden europea de producción.

¹¹ Memoria de la Fiscalía General del Estado 2024:
https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html

Cuando no es necesaria realizar notificación a la autoridad de ejecución, el destinatario deberá ejecutar la orden en el plazo máximo de 10 días a partir de la recepción de la orden. En caso de urgencia se cumplimentará en el plazo máximo de 8 horas.

Cuando se requiere notificar a la autoridad del Estado de ejecución, si en el plazo de 10 días la autoridad de ejecución no ha invocado un motivo de denegación, el destinatario remitirá la información al final del plazo de 10 días.

Si el destinatario considera que los datos solicitados están protegidos por inmunidades o privilegios concedidos en virtud del Derecho del Estado de ejecución o datos protegidos por normas de determinación o limitación de la responsabilidad penal relacionadas con la libertad de prensa y la libertad de expresión, informará sin demora a la autoridad emisora y a la autoridad de ejecución, en base a la información obtenida, la autoridad de emisión decidirá si mantiene, retira o adopta la orden. La autoridad de ejecución puede decidir oponer los motivos de denegación si se efectuó una notificación a la autoridad de ejecución con arreglo al artículo 8.

Si la orden está incompleta o contiene errores manifiestos o información insuficiente el destinatario informará sin demora a la autoridad emisora que realizará las aclaraciones que sean oportunas en el plazo máximo de 5 días. También el destinatario informará a la autoridad de ejecución cuando se le haya notificado la orden conforme al artículo 8.

Si el destinatario no puede cumplimentar la orden por circunstancias ajenas a su voluntad lo comunicará sin demora a la autoridad emisora que valorará si concurre o no dicha imposibilidad. También el destinatario informará a la autoridad de ejecución cuando se le haya notificado la orden conforme al artículo 8.

Cuando el destinatario no pueda entregar los datos por motivos distintos de los indicados informará a la autoridad emisora y, en su caso a la de ejecución y la autoridad emisora a la luz de la información recibida podrá establecer un nuevo plazo para la entrega de los datos.

El destinatario conservará los datos hasta su entrega o hasta que sea retirada la orden europea de producción. Cuando la conservación o la entrega no sea necesaria, la autoridad emisora informará al destinatario sin demora.

2. Orden europea de conservación.

El destinatario debe conservar los datos sin demora. La conservación de los datos se hará durante 60 días, prorrogables durante otros 30 días, salvo que la autoridad emisora dentro de dicho plazo haya emitido una solicitud posterior de entrega, en cuyo caso por el tiempo necesario para su ejecución.

Cuando la conservación no sea necesaria la autoridad emisora lo comunicará al destinatario y desde ese momento el deber de conservación cesará de inmediato.

De la misma forma que en las órdenes europeas de producción, si el destinatario considera que los datos están protegidos por inmunidades, privilegios, la libertad de prensa o de expresión; el destinatario informará a la autoridad emisora y a la de ejecución. La autoridad emisora decidirá si adapta, mantiene o retira la orden, por iniciativa propia o a petición de la autoridad de ejecución.

Si la orden está incompleta o contiene errores manifiestos o la información es insuficiente se informará a la autoridad emisora para que en el plazo de 5 días remita las aclaraciones

pertinentes. Si transcurren los 5 días sin que se haga la aclaración pertinente el prestador de servicios no estará obligado a cumplir la orden.

Cuando el destinatario no puede conservar los datos por hechos ajenos al mismo informara a la autoridad emisora explicando el motivo. Si la autoridad emisora considera que concurren informará al destinatario de que no hace falta cumplimentar la orden.

Si el destinatario no puede cumplimentar la orden por motivos distintos a los expuestos también se lo comunicará a la autoridad emisora para que a la luz de la motivación que realice el destinatario decidir si mantiene, adapta o retira la orden.

Con la finalidad de garantizar la efectividad de la cooperación jurídica internacional pretendida con el Reglamento y no hacer depender de la exclusiva voluntad del prestador de servicios el cumplimiento de la orden, en el artículo 16 del Reglamento se prevé que en caso de que el destinatario no facilite los datos requeridos y la autoridad de ejecución no haya invocado alguno de los motivos de denegación que estudiaremos a continuación, la autoridad emisora podrá requerir a la autoridad de ejecución que ejecute la orden de conservación o de producción.

La autoridad de ejecución reconocerá la orden en el plazo máximo de 5 días hábiles desde su recepción y tomará las medidas necesarias para la ejecución, salvo en los supuestos del apartado 4 y 5 del artículo 16 y que estudiaremos a continuación.

La autoridad de ejecución requerirá formalmente al destinatario para que cumpla con sus obligaciones y le informará de las sanciones aplicables en caso de incumplimiento y de la posibilidad de oponerse a la ejecución por alguno de los motivos siguientes.

El apartado 4 prevé los supuestos de denegación en caso de Orden Europea de Producción:

A. Defectos de emisión o competencia

1. a) No ha sido emitida o validada por autoridad competente con arreglo al Reglamento.
2. b) No se refiere a una infracción penal de las previstas en el Reglamento para amparar una orden.

B. Problemas materiales o técnicos

1. c) Imposibilidad de ejecución por causas ajenas al destinatario o existencia de errores manifiestos.
2. d) Los datos no estaban almacenados por el prestador en el momento de recibir la orden.
3. e) El servicio del destinatario no entra en el ámbito del Reglamento.

C. Límites jurídicos y garantías fundamentales

1. f) Datos protegidos por inmunidades o privilegios, o por normas sobre libertad de prensa y libertad de expresión.

2. g) Riesgo manifiesto de vulneración de un derecho fundamental (art. 6 TUE y Carta), basado en pruebas objetivas y basándose únicamente en la información de la orden europea de producción.

El apartado 5 prevé los motivos de denegación de la Orden Europea de Conservación

A. Defectos de emisión o competencia

1. a) No ha sido emitida o validada por autoridad competente con arreglo al Reglamento.

B. Problemas materiales o técnicos

- 1.b) Imposibilidad de ejecución por causas ajenas al destinatario o errores manifiestos.
- 2.c) Los datos no estaban almacenados por el prestador en el momento de recibir la orden.
- 3.d) El servicio no entra en el ámbito del Reglamento.

C. Límites jurídicos y garantías fundamentales

- e) Datos protegidos por inmunidades o privilegios, o por normas sobre libertad de prensa y libertad de expresión.
- f) Riesgo manifiesto de vulneración de un derecho fundamental (art. 6 TUE y Carta), basado en pruebas objetivas y solo con la información de la orden.

La autoridad de ejecución se pondrá en contacto con la autoridad emisora y podrá solicitar información adicional.

La autoridad de ejecución decidirá en base a la información obtenida del destinatario y la autoridad emisora. Una vez haya decidido sobre la ejecución lo notificará inmediatamente a la autoridad emisora y al destinatario.

Cuando obtenga los datos solicitados por la orden europea de producción, los transmitirá a la autoridad emisora sin demora.

Si el destinatario no cumple con la obligación que le incumbe cuando la ejecutoriedad ha sido reconocida por la autoridad de ejecución la autoridad impondrá una sanción pecuniaria de las previstas en el artículo 15. Contra la sanción pecuniaria debe haber recurso judicial efectivo.

7. Motivos de denegación.

La autoridad de ejecución es la competente de examinar si concurren motivos de denegación en los casos de la orden europea de producción cuando se pretenda la obtención de datos de tráfico (salvo los destinados a identificar al usuario) o de contenido.

De acuerdo con el artículo 12 los motivos de denegación son los siguientes:

- Que los datos solicitados estén protegidos por inmunidades o privilegios concedidos en virtud del Derecho del Estado de ejecución o datos protegidos por normas de determinación o limitación de la responsabilidad penal relacionadas con la libertad de prensa y la libertad de expresión.
- Cuando exista un riesgo de vulneración manifiesta de derechos fundamentales, siempre que existan pruebas objetivas que lo justifiquen.
- La ejecución de la orden sea contraria al principio *non bis in idem*.
- Cuando falte la doble incriminación, cuando la conducta que da origen a la orden no constituye delito en el Estado de ejecución ni esté recogido en el anexo IV, si en el Estado emisor está castigado con una pena o medida de seguridad privativas de libertad de una duración máxima no inferior a tres años.

La autoridad de ejecución tiene un plazo de 10 días, de 96 horas en caso de urgencia, a partir de la recepción de la notificación.

Antes de decidir la oposición del motivo de denegación, la autoridad de ejecución se comunicará con la autoridad emisora, que podrá optar entre retirar o adaptar la orden.

Si no se llega a un acuerdo y la autoridad de ejecución considera que concurre un motivo de denegación se lo comunicará a la autoridad emisora y a la autoridad destinataria. La autoridad destinataria interrumpirá la ejecución. La autoridad emisora retirará la orden.

Si la denegación es por razón de inmunidad o privilegio, se podrá interesar a la autoridad de ejecución que se ponga en contacto en su caso con la autoridad competente en el estado de ejecución para levantarla. Si la facultad para levantar la inmunidad o privilegio corresponde a la autoridad de otro Estado miembro o tercer país u organización internacional, la autoridad emisora podrá solicitar a la autoridad de que se trate que ejerza dicha facultad.

Además, de acuerdo con el art.1.3 del Reglamento, el mismo no podrá alterar la obligación de respetar los derechos fundamentales y los principios jurídicos establecidos en la Carta y en el artículo 6 del TUE, ni las obligaciones de las autoridades policiales o judiciales a este respecto, y se aplicará siempre sin perjuicio de principios fundamentales como la libertad de expresión e información —incluida la libertad y el pluralismo de los medios—, el respeto a la vida privada y familiar, la protección de datos personales y el derecho a la tutela judicial efectiva.

8. Sanciones

Con el fin de garantizar el cumplimiento de la orden de producción o de conservación y la efectividad de la cooperación judicial entre Estados, el Reglamento prevé la imposición de sanciones en caso de incumplimiento por los destinatarios de la orden.

Así las cosas, sin perjuicio de la posibilidad de que los derechos nacionales prevean sanciones penales, los Estados miembros deberán establecer un régimen de sanciones pecuniarias en caso de incumplimiento de la ejecución de la orden de producción, de conservación o en la adopción de medidas adecuadas para garantizar, la confidencialidad integridad y secreto de la orden y los datos obtenidos. Dichas sanciones deben ser

proporcionadas, eficaces y disuasorias, y pueden alcanzar hasta el 2 % del volumen de negocio mundial del prestador en el ejercicio anterior, lo que asegura que incluso las grandes plataformas tecnológicas perciban un impacto real. Además, los Estados miembros deben informar a la Comisión tanto del régimen adoptado como de cualquier modificación posterior. En este punto se echa en falta la unificación de la sanción aplicable al objeto de evitar situaciones de forum shopping donde los prestadores de servicios opten por establecerse en Estados con una régimen sancionador más laxo¹².

El artículo incorpora también una salvaguarda para los prestadores de servicios: no se les podrá exigir responsabilidad por los daños que puedan sufrir usuarios o terceros cuando estos deriven exclusivamente del cumplimiento de buena fe de una OEP o OEC. Con ello se evita que el cumplimiento de una obligación legal exponga a los proveedores a reclamaciones civiles injustificadas que les disuadan de dar cumplimiento a las órdenes.

9. Derechos de la persona cuyos datos se solicitan.

El Reglamento prevé dos derechos básicos de la persona cuyos datos son solicitados: el derecho a ser informado y el derecho a recurrir la orden.

El artículo 13 del Reglamento establece que la persona cuyos datos se solicitan mediante una orden europea de producción debe ser informada por la autoridad emisora sin demora, salvo que existan razones legales para retrasar, limitar u omitir esa comunicación, como la protección de una investigación, la seguridad pública, seguridad nacional o proteger los derechos y libertades de otras personas. Cuando se informe al afectado, deben indicarse también las vías de recurso disponibles. Además, tanto el destinatario de la orden como el prestador de servicios deben aplicar medidas técnicas y operativas avanzadas para garantizar la confidencialidad, el secreto y la integridad de la orden y de los datos.

Por su parte, el artículo 18 prevé que sin perjuicio de otras posibles vías de conformidad con el Derecho Nacional, toda persona cuyos datos hayan sido solicitados mediante una orden de producción tendrá derecho a vías de recurso efectivas contra dicha orden. Si esa persona sospechosa o acusada, tendrá derecho a vías de recurso efectivas en el proceso penal donde se usen los datos. Ello sin perjuicio del derecho a la tutela judicial efectiva con arreglo al Reglamento 2016/679 y la Directiva (UE) 2016/680.

El recurso se ejercerá ante un órgano jurisdiccional del Estado emisor y deberá incluir la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la medida, sin perjuicio de las garantías de los derechos fundamentales en el Estado de ejecución.

Además, el Estado emisor y cualquier otro Estado donde se remitan las pruebas electrónicas obtenidas velarán porque se respeten los derechos de defensa y equidad del proceso al valorar las pruebas obtenidas a través de la orden europea de producción.

También se reconoce el derecho a la persona acusada o investigada en un procedimiento penal de promover la emisión de la orden, recogiendo que la emisión de la orden se podrá realizar a instancia de la persona sospechosa o acusada o por un abogado en

¹² MURIEL DIÉGUEZ J.A. Implicaciones del Reglamento (UE) sobre órdenes europeas de entrega y conservación de pruebas electrónicas y la Directiva (UE) 2023/1544 en el proceso penal. *Revista Electrónica de Direito. Universidade Do Porto*, octubre de 2024, nº 3.

nombre de dicha persona, en el marco de los derechos de defensa aplicables de conformidad con el Derecho procesal penal nacional.

10. Conflicto de leyes.

El artículo 17 del Reglamento (UE) 2023/1543 introduce un mecanismo específico para resolver los conflictos que pueden surgir cuando la ejecución de una Orden Europea de Producción (OEP) entra en conflicto con una obligación jurídica impuesta por el Derecho aplicable de un tercer país. Esta previsión responde a la necesidad de equilibrar la eficacia de la cooperación judicial penal en la Unión con el respeto de los derechos fundamentales, las obligaciones internacionales y los intereses esenciales de Estados no miembros.

El procedimiento se activa cuando el destinatario de la OEP considera que cumplir la orden le obligaría a infringir una norma aplicable de un país tercero. En ese caso, el artículo 17 exige que el prestador de servicios presente la objeción motivada tanto a la autoridad emisora como a la autoridad de ejecución, dentro del plazo general de diez días previsto para la respuesta a las órdenes. Esa objeción debe explicar con precisión qué norma extranjera resulta aplicable, por qué lo es en el caso concreto y cuál es la obligación en conflicto. El Reglamento deja claro que no basta alegar que el tercer país carece de normas equivalentes a las órdenes de producción o que los datos se encuentran físicamente almacenados allí.

Una vez recibida la objeción, la autoridad emisora debe examinarla, teniendo en cuenta también las observaciones del Estado de ejecución. Si, tras ese análisis, la autoridad emisora mantiene su intención de confirmar la OEP, el artículo 17 prevé que la autoridad emisora solicite un reexamen al órgano jurisdiccional competente del Estado emisor. Durante este reexamen, la ejecución de la orden queda suspendida, lo que garantiza que no se vulneren derechos fundamentales ni se incumplan obligaciones internacionales mientras se resuelve el conflicto.

El órgano jurisdiccional debe determinar, en primer lugar, si la legislación del tercer país es realmente aplicable al caso concreto y, en segundo lugar, si esa legislación prohíbe efectivamente la divulgación de los datos solicitados. Si cualquiera de estas dos condiciones no se cumple, la OEP se confirmará sin necesidad de mayor ponderación.

Sin embargo, si el tribunal concluye que existe una prohibición real derivada del Derecho extranjero, el artículo 17 exige una ponderación detallada de diversos factores antes de decidir si confirma o retira la orden. Entre esos factores se encuentran la importancia de los intereses protegidos por el derecho extranjero incluidos los derechos e intereses fundamentales que impidan la revelación de los datos y en particular los intereses de seguridad nacional de tercer país; y la conexión de la causa penal para la que se ha emitido la orden y el país tercero, valorando entre otros la ubicación de los datos, la nacionalidad o residencia de la persona cuyos datos se solicitan o de la víctima de la infracción de que se trate, el lugar en el que se haya cometido el delito, la relación del proveedor de servicios con ese país, los intereses del Estado investigador en función de la gravedad de la infracción y la importancia de la obtención de las pruebas con prontitud y las posibles consecuencias para el destinatario o prestador de servicios si cumple con la orden incluidas las posibles sanciones. Esta ponderación refleja el equilibrio que el Reglamento busca entre la eficacia de la cooperación judicial y el respeto de las obligaciones internacionales.

El artículo 17 también contempla la posibilidad de que el órgano jurisdiccional solicite información adicional a las autoridades del tercer Estado, siempre que ello no perjudique el procedimiento penal en curso. En todo caso solicitara información del tercer Estado cuando el conflicto de obligaciones afecte a derechos fundamentales u otros intereses fundamentales del tercer país relacionados con la seguridad nacional y la defensa. Esta facultad resulta especialmente relevante cuando están en juego derechos fundamentales o cuestiones de seguridad nacional, y se integra en el marco general de cooperación internacional previsto en el Reglamento.

Una vez adoptada la decisión, el órgano jurisdiccional la comunicará a la autoridad emisora y al destinatario. Los plazos aplicables se rigen por el Derecho nacional del Estado emisor.

A través de la objeción motivada, el reexamen judicial y la ponderación de intereses, el Reglamento asegura que la cooperación judicial transfronteriza en materia penal se desarrolle dentro de un marco equilibrado, respetuoso con el principio de legalidad y con los intereses legítimos de todas las partes implicadas.

A pesar de ello no debe dejar de criticarse el modo en que está redactado el precepto puesto que plantea dudas a la hora de determinar quien será el órgano jurisdiccional competente para hacer el reexamen.

El Reglamento distingue claramente entre la autoridad emisora y el órgano jurisdiccional, lo que sugiere que no deben coincidir. De hecho, la propia expresión “la autoridad emisora (...) solicitará un reexamen por el órgano jurisdiccional competente del Estado emisor” transmite la idea de que se trata de un ente distinto de la autoridad emisora, lo que cobra especial sentido cuando la OEP ha sido emitida por el Ministerio Fiscal, que no es un órgano jurisdiccional.

El problema surge cuando la OEP la emite un juez. El Reglamento no aclara si ese mismo juez puede revisar su propia decisión o si debe hacerlo un órgano superior. Desde una perspectiva garantista, lo coherente sería que el reexamen lo realizara un órgano distinto, pues de lo contrario el control judicial perdería parte de su sentido: un juez revisando su propia orden difícilmente puede ofrecer el mismo grado de imparcialidad que un órgano revisor independiente. Sin embargo, el Derecho español no ha desarrollado aún una norma que determine expresamente qué órgano debe asumir esta función.

El mecanismo de control del artículo 17 tiene su homónimo en la cláusula de cortesía de la CLOUD ACT, en virtud de la cual los proveedores de servicios pueden pedir al tribunal competente en Estados Unidos que anule o modifique una orden de entrega o protección de datos cuando los datos pertenezcan a una persona que no sea estadounidense y cumplir la orden supondría violar la ley de otro país que tenga un acuerdo oficial con Estados Unidos, el cual ofrezca a los proveedores del otro país un derecho similar para proteger sus datos según sus propias leyes¹³.

11. La designación de establecimientos y representantes legales para recabar las pruebas electrónicas.

¹³ Nota de la Presidencia al Consejo de la Unión Europea, de 28 de mayo de 2018 (9418/18): <https://data.consilium.europa.eu/doc/document/ST-9418-2018-INIT/es/pdf>

La aprobación del Reglamento 2023/1543 vino acompañada de la Directiva 2023/1544, que debía trasponerse antes del 18 de febrero de 2026.

La Directiva (UE) 2023/1544 constituye un instrumento esencial para adaptar la cooperación judicial penal a un entorno digital en el que la ubicación física de los datos no limite la obtención de pruebas. Su arquitectura se apoya en tres principios de efectividad, cooperación leal y responsabilidad empresarial en el entorno digital, que permiten superar los obstáculos territoriales tradicionales y obliga a los prestadores de servicios a integrarse de forma activa y jurídicamente responsable en el funcionamiento del proceso penal europeo.

Sobre esta base, los artículos 2 a 6 articulan un sistema que combina las obligaciones del establecimiento o representante legal en la Unión, la responsabilidad solidaria, un régimen sancionador armonizado y la intervención de autoridades centrales. Este entramado normativo asegura que las órdenes de producción o conservación de datos puedan ejecutarse con rapidez y seguridad, equilibrando la libertad de prestación de servicios digitales con las exigencias del proceso penal y configurando un modelo de corresponsabilidad entre operadores privados y autoridades públicas.

La Directiva tiene por objeto que los Estados miembros velen porque los prestadores de servicios que ofrezcan servicios en la Unión designen establecimientos y representantes legales para el cumplimiento y la ejecución de órdenes emitidas al amparo del Reglamento 2023/1543 y la Directiva 2014/41/UE y y de cualquier convenio aplicable celebrado por el Consejo, de conformidad con el artículo 34 del Tratado de la Unión Europea.

La Directiva también se aplica a las resoluciones y órdenes que emitan las autoridades de un Estado miembro a prestadores de servicios establecidos en su territorio para obtener prueba electrónica en un proceso penal y sin perjuicio de las competencias atribuidas a las autoridades competentes por el derecho nacional y el derecho de la Unión para dirigirse a los prestadores de servicios establecidos en su territorio directamente.

En la Directiva se prevé que los Estados no impondrán obligaciones adicionales a las previstas en la misma en particular en lo que se refiere a la designación de establecimientos designados o representantes legales.

No se aplica a los prestadores de servicios establecidos en un único Estado miembro que presten servicios solo a dicho Estado miembro.

Por prestador de servicios debe entenderse toda persona física o jurídica que preste determinados servicios digitales, excluyendo expresamente los regulados en la Directiva 2006/123/CE.

Son servicios digitales los servicios de comunicaciones electrónicas, los servicios de nombres de dominio IP, registro de nombre de dominio, registrador de nombres de dominio y servicios de privacidad y representación relacionados con nombres de dominio; y otros servicios de la sociedad de la información que permitan la comunicación entre usuarios, o impliquen tratamiento o almacenamiento de datos como componente esencial del servicio.

Se entiende que prestan servicios en un Estado miembro o en la Unión cuando permitan el uso a personas físicas y jurídicas en un Estado miembro o cuando tengan una conexión sustancial con un Estado miembro, por ejemplo por tener un establecimiento en dicho Estado o cuando exista un número significativo de usuarios en dicho Estado miembro u

oriente su actividad hacia dicho Estado miembro. En el considerando 10 de la Directiva se indica que la evaluación sobre si un proveedor está ofreciendo servicios dentro de la Unión Europea requiere analizar si realmente permite que personas —ya sean particulares o empresas— situadas en uno o varios Estados miembros utilicen esos servicios. Sin que el hecho de que una interfaz en línea sea accesible desde la Unión —por ejemplo, que una página web pueda abrirse desde Europa o que aparezca un correo electrónico u otros datos de contacto del proveedor o de un intermediario— baste por sí solo para concluir que dicho proveedor está ofreciendo servicios en la UE.

En función de si el prestador de servicios está establecido o no en la Unión los Estados miembros velarán porque el prestador de servicios designe un establecimiento en el primer caso o a un representante legal en el segundo. Los establecimientos designados o representantes legales actuarán como destinatarios de las órdenes europeas de producción o conservación de pruebas. Se impone así una arquitectura de responsabilidad territorial que impide la evasión por razón de localización empresarial.

Los Estados miembros también velarán porque los prestadores de servicios establecidos en su territorio o que ofrezcan servicios en él, doten a los establecimientos designados o representantes legales de competencias y recursos suficientes para cumplir con las órdenes europeas recibidas de un Estado miembro. Además, los Estados verificarán que se les ha dotado de dichas competencias, recursos y que cooperen.

Al objeto de garantizar la efectividad del Reglamento y evitar que la descentralización de un prestador de servicios sirva de pretexto para eludir las obligaciones que le competen, la Directiva prevé un sistema de responsabilidad solidaria entre el prestador de servicios y el establecimiento designado o el representante legal al objeto de evitar que pueda utilizarse la falta de procedimientos internos adecuados como justificación de incumplimiento de sus obligaciones.

Con la misma finalidad la Directiva prevé que los Estados miembros velarán por que cada prestador de servicios establecido en su territorio o que preste servicios en él facilite a la autoridad central designada los datos de contacto del establecimiento designado o representante legal. En la información que deben facilitar a la autoridad central, deberán indicar las lenguas en que podrán comunicarse con el establecimiento designado o representante legal y el ámbito territorial de la designación de dichos establecimientos o representantes legales.

Se prevé la publicación en una página específica de la Red Judicial Europea en materia penal, reforzando la transparencia y la accesibilidad para las autoridades competentes.

En caso de incumplimiento de las disposiciones nacionales adoptadas al amparo de lo ya expuesto se prevé que los Estados establezcan un régimen de sanciones que sean efectivas, proporcionadas y disuasorias

12. El sistema descentralizado europeo.

El Reglamento (UE) 2023/1543 prevé la creación de un sistema informático descentralizado destinado a garantizar la cooperación digital entre autoridades y prestadores de servicios en el marco de las órdenes europeas de producción y conservación de pruebas electrónicas. Dicho sistema permite el intercambio electrónico

transfronterizo de formularios, datos e información de forma rápida, directa, interoperable, sostenible, fiable y segura.

El propio Reglamento define el sistema informático descentralizado como una red de sistemas informáticos y puntos de acceso interoperables que opera bajo la responsabilidad y gestión individual de cada Estado miembro, agencia u organismo de la Unión, y que permite el intercambio transfronterizo de información de forma segura y fiable.

En virtud de este marco, las comunicaciones escritas entre las autoridades competentes y los establecimientos designados o representantes legales de los prestadores de servicios deben realizarse, con carácter general, a través de dicho sistema. Se establece así un modelo de corresponsabilidad institucional, en el que los Estados miembros deben garantizar el funcionamiento del sistema para las autoridades destinatarias, mientras que los prestadores de servicios deben asegurar que sus establecimientos designados o representantes legales puedan utilizarlo eficazmente.

No obstante, el Reglamento admite excepciones al uso del sistema informático descentralizado cuando existan circunstancias técnicas, jurídicas o forenses que impidan su utilización, como interrupciones del sistema, limitaciones técnicas relacionadas con el tamaño de los datos, requisitos relativos a la admisibilidad probatoria o circunstancias excepcionales. En tales casos, la comunicación podrá efectuarse mediante el medio alternativo más seguro y verificable disponible, debiendo registrarse posteriormente en el sistema a fin de garantizar la trazabilidad del intercambio.

Con el objetivo de concretar los aspectos técnicos y operativos del sistema, la Comisión adoptó el Reglamento de Ejecución (UE) 2025/1550, que establece las especificaciones técnicas y los requisitos de funcionamiento del sistema informático descentralizado. Su relevancia radica en que transforma el mandato normativo del Reglamento en un sistema operativo concreto, basado en estándares técnicos verificables.

El sistema se configura como una red de sistemas nacionales interconectados mediante puntos de acceso basados en e-CODEX, lo que garantiza la interoperabilidad entre las infraestructuras informáticas de los distintos Estados miembros. Asimismo, el Reglamento de Ejecución fija, como regla general, un umbral de 25 MB para la transmisión de pruebas electrónicas a través del sistema; cuando los datos superen dicho límite, deberán transmitirse por medios alternativos, debiendo registrarse posteriormente la transmisión en el sistema nacional o de la Unión para asegurar la trazabilidad y autenticidad de la cooperación.

Desde el punto de vista técnico, el sistema debe apoyarse en protocolos y estándares ampliamente aceptados, incluyendo servicios web basados en arquitecturas SOAP o REST, protocolos de mensajería segura como AS4 o interfaces API seguras (HTTPS/REST), así como mecanismos de autenticación y cifrado basados en estándares como TLS, OpenID Connect o infraestructuras de clave pública con firmas digitales.

El Reglamento de Ejecución también establece un conjunto de medidas técnicas mínimas de seguridad informática, destinadas a garantizar la confidencialidad de las comunicaciones mediante canales seguros, el no repudio del origen y de la recepción de la información, la disponibilidad de los servicios y datos, el registro de incidentes de seguridad, la autenticación y autorización de los usuarios y la verificación de la identidad de los sistemas conectados.

La Comisión Europea es responsable del desarrollo y mantenimiento del programa informático de aplicación de referencia, que debe cumplir plenamente las normas europeas de protección de datos. Los Estados miembros que opten por utilizar sistemas propios deberán garantizar igualmente el cumplimiento del Reglamento (UE) 2016/679 y de la Directiva (UE) 2016/680. Asimismo, los Estados miembros, Eurojust y la Fiscalía Europea deberán disponer de mecanismos sólidos de seguridad destinados a detectar y responder a incidentes en los sistemas que integran el sistema informático descentralizado.

Finalmente, el Reglamento establece objetivos concretos de disponibilidad del sistema. Los Estados miembros, Eurojust y la Fiscalía Europea deberán garantizar la disponibilidad de los componentes bajo su responsabilidad veinticuatro horas al día y siete días a la semana, con una tasa mínima de disponibilidad técnica del 98 % anual, excluido el mantenimiento programado. Por su parte, la Comisión deberá garantizar la disponibilidad de la base de datos central con un objetivo superior al 99 % anual, previéndose que las operaciones de mantenimiento se realicen preferentemente entre las 20:00 y las 7:00 horas (CET).

Además, el sistema incorpora una base de datos estructurada que contiene información sobre autoridades competentes y proveedores de servicios, con el fin de permitir el enrutamiento correcto de las comunicaciones. Esta base de datos incluye datos de identificación, competencias territoriales, contactos técnicos y parámetros necesarios para el direccionamiento automático de mensajes. La Comisión es responsable de su desarrollo y mantenimiento, mientras que los Estados miembros deben garantizar que la información esté completa, sea exacta y se mantenga permanentemente actualizada.

13. Conclusiones

El estudio del Reglamento (UE) 2023/1543 muestra que la Unión Europea ha optado por un modelo de cooperación judicial adaptado a la realidad tecnológica actual, donde la rapidez y la disponibilidad de los datos son esenciales para la eficacia de las investigaciones penales. La comunicación directa con los prestadores de servicios, que constituye la principal innovación del sistema, permite superar la lentitud de los mecanismos clásicos, aunque introduce nuevas tensiones en materia de garantías y control jurisdiccional.

Pese a estas críticas, el Reglamento incorpora contrapesos relevantes: notificación obligatoria al Estado de ejecución en los supuestos más invasivos, mecanismos de denegación, intervención judicial en caso de conflicto de leyes y un sistema sancionador que asegura el cumplimiento. La Directiva 2023/1544 complementa este marco al imponer la designación de establecimientos o representantes legales, reforzando la responsabilidad empresarial en la cooperación penal europea.

En conjunto, el Reglamento y su normativa asociada configuran un sistema más funcional y coherente con la naturaleza transnacional de la evidencia digital, aunque su eficacia dependerá de la correcta articulación entre autoridades nacionales, prestadores de servicios y órganos jurisdiccionales. El reto futuro será garantizar que la agilidad no erosione las garantías procesales y que la cooperación internacional mantenga un equilibrio adecuado entre eficacia investigadora y protección de derechos fundamentales.

Bibliografía

- CUADRADO SALINAS, C. La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?. *IUS ET SCIENTIA*, 2023, Vol.9 nº2.
- DELGADO MARTÍN, J. Prueba digital internacional. El Reglamento E-Evidence. *Revista La Ley, Sección Ciberderecho*, 15 de septiembre de 2023, nº76.
- DE HOYOS SANCHO, M. *REVISTA DE ESTUDIOS EUROPEOS*, Universidad de Valladolid, 2023, n.º Extraordinario monográfico 1
- ESPINA RAMOS J. A. *European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU. Implications of the Union Legislator's Choice to Derogate from the Precedence of Union Law in the E-Evidence Regulation*. *Eucrim*. 2025, Vol. 20(3).
- ESTÉVEZ BENITO R. La conservación y acceso a las evidencias digitales más allá de la Unión Europea. El Convenio de Budapest y sus dos Protocolos Adicionales. *Diario La Ley, Sección Ciberderecho*, nº103, 23 de febrero de 2026.
- GÓMEZ AMIGO L. Estudio de las órdenes europeas de producción y conservación: un instrumento para la obtención transfronteriza de pruebas penales electrónicas. *Revista Española de Derecho Europeo*, octubre-diciembre de 2024, nº 92.
- MURIEL DIÉGUEZ J.A. Implicaciones del Reglamento (UE) sobre órdenes europeas de entrega y conservación de pruebas electrónicas y la Directiva (UE) 2023/1544 en el proceso penal. *Revista Electrónica de Direito. Universidad Do Porto*, octubre de 2024, nº 3.
- TINOCO PASTRANA A. Las órdenes europeas de producción y de conservación de prueba electrónica transfronteriza en los procesos penales en la Unión Europea. *Revista de Estudios Europeos*, 2025, nº86.

Enlaces

- El Convenio sobre la Ciberdelincuencia: <https://eur-lex.europa.eu/ES/legal-content/summary/convention-on-cybercrime.html>
- La orden europea de investigación, asistencia judicial mutua y equipos conjuntos de investigación: https://e-justice.europa.eu/topics/court-procedures/criminal-cases/judicial_cooperation/european-investigation-order-mutual-legal-assistance-and-joint-investigation-teams_es
- The Cloud Act: <https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf>
- Memoria de la Fiscalía General del Estado 2024:
https://www.fiscal.es/memorias/memoria2024/FISCALIA_SITE/index.html

-Nota de la Presidencia al Consejo de la Unión Europea, de 28 de mayo de 2018 (9418/18):
<https://data.consilium.europa.eu/doc/document/ST-9418-2018-INIT/es/pdf>

-The EU Electronic Evidence Legislative Package Annual Report:
<https://www.eurojust.europa.eu/sites/default/files/assets/files/sirius-e-evidence-legislative-package-annual-report.pdf>

-Recomendación de DECISIÓN DEL CONSEJO por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52019PC0070>