Consejo de la Unión Europea

Bruselas, 18 de abril de 2018
(OR. en)

8110/18

Expediente interinstitucional: 2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PROPUESTA

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	18 de abril de 2018
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2018) 225 final
Asunto:	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal

Adjunto se remite a las Delegaciones el documento – COM(2018) 225 final.

Adj.: COM(2018) 225 final

COMISIÓN
EUROPEA

Estrasburgo, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal

{SWD(2018) 118 final} - {SWD(2018) 119 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

• Motivos y objetivos de la propuesta

En la actualidad, la utilización de las redes sociales, los servicios de correo electrónico y de mensajería y las aplicaciones para comunicarse, trabajar, crear lazos sociales y obtener información se ha convertido en algo habitual en muchas partes del mundo. Estos servicios conectan entre sí a cientos de millones de usuarios y generan importantes beneficios para el bienestar social y económico de los usuarios en la Unión y fuera de ella. Sin embargo, también se pueden utilizar indebidamente como instrumentos para cometer o facilitar delitos graves, en particular atentados terroristas. Cuando esto sucede, dichos servicios y aplicaciones son a menudo el único lugar donde los investigadores pueden hallar pistas para determinar quién ha cometido un delito y obtener pruebas que puedan utilizarse ante los tribunales.

Dado que internet no conoce fronteras, estos servicios pueden prestarse desde cualquier lugar del mundo y no exigen necesariamente una infraestructura física ni una presencia empresarial o personal en los Estados miembros en los que se ofrecen o en el mercado interior en su conjunto. Tampoco requieren una ubicación específica para el almacenamiento de los datos, que a menudo es elegida por el proveedor de servicios sobre la base de consideraciones legítimas como la seguridad de los datos, las economías de escala y la rapidez de acceso. En consecuencia, en un número creciente de casos penales relativos a todo tipo de delitos[1], las autoridades de los Estados miembros necesitan acceder a datos que puedan servir como prueba y que están almacenados fuera de su país o por proveedores de servicios de otros Estados miembros o de países terceros.

Para situaciones en que las pruebas o el proveedor de servicios están ubicados en otro lugar, ya se desarrollaron hace varios decenios mecanismos de cooperación entre países[2]. A pesar de las frecuentes reformas, estos mecanismos de cooperación están sometidos a una presión creciente debido a la mayor necesidad de poder acceder rápidamente a pruebas electrónicas de forma transfronteriza. En respuesta, varios Estados miembros y países terceros han recurrido a la ampliación de sus herramientas nacionales; la consiguiente fragmentación genera inseguridad jurídica y obligaciones contradictorias y plantea la cuestión de la protección de los derechos fundamentales y las garantías procesales de las personas afectadas por tales solicitudes.

En 2016, el Consejo pidió acciones concretas basadas en un enfoque común de la UE para una asistencia jurídica mutua más eficaz, para mejorar la cooperación entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE y para proponer soluciones al problema de la determinación y aplicación de la jurisdicción[3] en el ciberespacio[4]. El Parlamento Europeo también puso de relieve los retos que el actualmente fragmentado marco jurídico puede suponer para los proveedores de servicios

---

1 Véanse los apartados 2.1.1 y 2.3 de la evaluación de impacto.

2 En la Unión, los mecanismos de reconocimiento mutuo se basan actualmente en la Directiva sobre la orden europea de investigación; con países terceros se recurre a mecanismos de asistencia judicial mutua.

3 En el presente documento, el término «jurisdicción de ejecución» se refiere a la competencia de las autoridades pertinentes para abrir una investigación.

4 Conclusiones del Consejo de la Unión Europea sobre la mejora de la justicia penal en el ciberespacio, ST9579/16.

que desean dar cumplimiento a los requerimientos legales e hizo un llamamiento en favor de un marco jurídico europeo que incluya salvaguardias para los derechos y las libertades de los interesados[5].

La presente propuesta aborda el problema específico derivado del carácter volátil de las pruebas electrónicas y su dimensión internacional. Intenta adaptar los mecanismos de cooperación a la era digital, ofreciendo a las autoridades judiciales y policiales herramientas para abordar la forma en que los delincuentes se comunican en la actualidad, y para luchar contra las nuevas formas de delincuencia. Estos instrumentos están ligados a unos sólidos mecanismos de protección de los derechos fundamentales. La presente propuesta tiene por objeto mejorar la seguridad jurídica para las autoridades, los proveedores de servicios y las personas afectadas, y mantener un nivel elevado por lo que respecta a las solicitudes de las autoridades competentes, asegurando así la protección de los derechos fundamentales, la transparencia y la responsabilidad. También acelera el proceso para obtener y asegurar pruebas electrónicas que estén almacenadas o que obren en poder de proveedores de servicios establecidos en otra jurisdicción. Este instrumento coexistirá con los actuales instrumentos de cooperación judicial, que siguen siendo pertinentes y pueden ser utilizados, en su caso, por las autoridades competentes. Paralelamente, la Comisión está trabajando para reforzar los mecanismos de cooperación judicial existentes a través de medidas como la creación de una plataforma segura para el intercambio rápido de solicitudes entre autoridades judiciales de la Unión y la inversión de 1 millón EUR para formar a profesionales de todos los Estados miembros de la UE en materia de asistencia judicial y cooperación, prestando especial atención a los Estados Unidos, pues se trata del país tercero que recibe el mayor número de solicitudes procedentes de la UE[6].

Para la notificación y ejecución de órdenes en virtud de este instrumento, las autoridades deben recurrir al representante legal designado por el proveedor de servicios. La Comisión presenta hoy una propuesta para garantizar que dichos representantes legales sean efectivamente designados. Se aporta así una solución común a escala de la UE para transmitir órdenes a los proveedores de servicios por medio de un representante legal.

- **Coherencia con las disposiciones vigentes de la UE en este ámbito y con el Convenio de Budapest del Consejo de Europa**

El actual marco jurídico de la UE consta de instrumentos de cooperación de la Unión en materia penal, como la Directiva 2014/41/UE relativa a la orden europea de investigación en materia penal[7], el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea[8], la Decisión 2002/187/JAI del Consejo por la que se crea Eurojust[9], el Reglamento (UE) 2016/794 sobre Europol[10], y la Decisión marco 2002/465/JAI

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, DO L 130 de 1.5.2014, p. 1.

8 Acto del Consejo, de 29 de mayo de 2000, por el que se establece, de conformidad con el artículo 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea.

9 Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia. En 2013, la Comisión adoptó una propuesta de Reglamento por el que se reforma Eurojust [Propuesta de Reglamento del Parlamento Europeo y del

del Consejo sobre equipos conjuntos de investigación[11], así como de acuerdos bilaterales entre la Unión y países terceros, como el Acuerdo de Asistencia Judicial Mutua entre la UE y Estados Unidos[12] y el Acuerdo de Asistencia Judicial entre la Unión Europea y Japón[13].

Mediante la introducción de la orden europea de entrega y la orden europea de conservación, la propuesta facilita asegurar y recabar, a efectos de procesos penales, pruebas electrónicas que se encuentran almacenadas o conservadas por los proveedores de servicios en otra jurisdicción. La Directiva relativa a la orden europea de investigación en materia penal, que en gran parte sustituyó al Convenio de Asistencia Judicial en Materia Penal, cubre todas las medidas de investigación[14], incluido el acceso a las pruebas electrónicas, pero no contiene disposición específica alguna sobre este tipo de pruebas[15]. El nuevo instrumento no sustituirá a dicha Directiva a efectos de obtener pruebas electrónicas, pero ofrece un instrumento adicional a las autoridades. Puede ocurrir, por ejemplo, que varias medidas de investigación deban ejecutarse en el Estado miembro de ejecución, en cuyo caso la susodicha Directiva puede ser la opción preferida por las autoridades públicas. La creación de un nuevo instrumento para las pruebas electrónicas es una mejor alternativa que modificar la Directiva, debido a los problemas específicos inherentes a la obtención de pruebas electrónicas, que no afectan a las otras medidas de investigación cubiertas por la Directiva relativa a la orden europea de investigación en materia penal.

Para facilitar la obtención transfronteriza de pruebas electrónicas, el nuevo instrumento se basa en los principios de reconocimiento mutuo. Una autoridad del país en el que esté establecido el destinatario de la orden no tendrá que intervenir directamente en la notificación y ejecución de la orden, salvo si existe incumplimiento, en cuyo caso se exigirá la ejecución y entonces intervendrá la autoridad competente del país en el que esté establecido el representante. Por ello, el instrumento requiere una serie de sólidas salvaguardias y disposiciones, como la validación por una autoridad judicial en cada caso. Por ejemplo, las órdenes europeas de entrega de datos de transacciones o de datos de contenido (por oposición a los datos de los abonados y los datos relativos al acceso) pueden ser emitidas únicamente con respecto a delitos punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años, o con respecto a delitos específicos relacionados con el ciberespacio o cometidos mediante la utilización del ciberespacio, o con respecto a delitos de terrorismo contemplados en la propuesta.

Consejo sobre la Agencia Europea de Cooperación en materia de Justicia Penal (Eurojust), COM(2013) 535 final].

10 Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI.

11 Decisión marco 2002/465/JAI del Consejo, de 13 de junio de 2002, sobre equipos conjuntos de investigación.

12 Decisión 2009/820/PESC del Consejo, de 23 de octubre de 2009, sobre la celebración, en nombre de la Unión Europea, del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América y del Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos de América.

13 Decisión 2010/616/UE del Consejo, de 7 de octubre de 2010, relativa a la celebración del Acuerdo entre la Unión Europea y Japón sobre asistencia judicial en materia penal.

14 A excepción de los equipos conjuntos de investigación (véase el artículo 3 de Directiva); no todos los Estados miembros participan en la Directiva (Irlanda y Dinamarca).

15 A excepción de una referencia a la identificación del titular de una dirección IP en el artículo 10, apartado 2, letra e), para el cual no podrá invocarse la doble tipificación como motivo de denegación del reconocimiento y la ejecución de la solicitud.

Los datos personales cubiertos por la presente propuesta están protegidos y solo podrán ser tratados de conformidad con el Reglamento general de protección de datos[16] y la Directiva protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes[17]. El Reglamento general de protección de datos entrará en vigor el 25 de mayo de 2018, mientras que la Directiva sobre protección de datos tiene que ser transpuesta por los Estados miembros a más tardar el 6 de mayo de 2018.

El Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia (STCE n.º 185), ratificado por la mayoría de los Estados miembros de la UE, establece mecanismos internacionales de cooperación en la lucha contra la ciberdelincuencia[18]. El Convenio versa sobre los delitos cometidos a través de internet y otras redes informáticas. Además, obliga a las Partes a establecer competencias y procedimientos para la obtención de pruebas electrónicas y a prestarse mutuamente asistencia jurídica, sin limitarse a los delitos informáticos. En particular, exige a las Partes que establezcan una orden de entrega para obtener datos informáticos que obren en poder de los proveedores de servicios en su territorio y datos de los abonados que obren en poder de los proveedores que presten servicios en su territorio. Asimismo, el Convenio contempla las órdenes de conservación de datos cuando existan motivos para pensar que los datos informáticos son especialmente vulnerables a pérdidas o modificaciones. La notificación y la ejecutabilidad de las órdenes nacionales de entrega frente a proveedores establecidos fuera del territorio de una Parte del Convenio plantean nuevos problemas. En este sentido, todavía están en fase de estudio nuevas medidas para mejorar el acceso transfronterizo a las pruebas electrónicas[19].

- **Resumen de la propuesta de Reglamento**

La propuesta de Reglamento introduce órdenes europeas vinculantes de entrega y conservación de datos. Ambas órdenes deben ser emitidas o validadas por una autoridad judicial de un Estado miembro. Puede emitirse una orden para solicitar la conservación o la entrega de datos almacenados por un proveedor de servicios de pago ubicado en otra jurisdicción y que sean necesarios como prueba en investigaciones o procesos penales. Estas órdenes solo podrán emitirse si existe una medida similar para la misma infracción en una situación comparable a nivel nacional en el Estado emisor. Ambas órdenes pueden ser notificadas a proveedores de servicios de comunicaciones electrónicas, redes sociales y mercados en línea, a otros proveedores de servicios de alojamiento de datos en internet, y a proveedores de infraestructuras, tales como registros de nombres de dominio y de direcciones

16 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

17 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

18 En la Estrategia de Ciberseguridad de la Unión Europea de 2013, el Convenio de Budapest fue reconocido como el principal marco multilateral para la lucha contra la ciberdelincuencia - Comunicación conjunta de la Comisión y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad sobre una Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, JOIN(2013) 1 final.

19 En su 17.º Pleno (junio de 2017), el Comité del Convenio sobre la Ciberdelincuencia aprobó el mandato para la preparación de un segundo Protocolo adicional del Convenio (Segundo Protocolo Adicional), que deberá estar preparado y ultimado por dicho Comité en diciembre de 2019. El objetivo de abandonar el emplazamiento del almacenamiento de datos es un factor determinante.

IP, o a sus representantes legales, cuando existan. La orden europea de conservación, de forma similar a la orden europea de entrega, se remite al representante legal fuera de la jurisdicción del Estado miembro emisor a efectos de conservar los datos en vista de una solicitud posterior para entregarlos, por ejemplo mediante la asistencia judicial en caso de países terceros o a través de una orden europea de investigación entre los Estados miembros participantes. A diferencia de las medidas de vigilancia o las obligaciones de conservación de datos estipuladas por ley, que no están previstas en el presente Reglamento, la orden europea de conservación es emitida o validada por una autoridad judicial en un proceso penal concreto tras una evaluación individual de la proporcionalidad y necesidad en cada caso. Al igual que la orden europea de entrega, se refiere a los autores específicos, conocidos o desconocidos, de una infracción penal que ya ha ocurrido. La orden europea de conservación solo permite conservar datos que ya se encuentren almacenados en el momento de la recepción de la orden, no acceder a datos en un momento futuro tras la recepción de la orden.

Ambas órdenes solo pueden utilizarse en procesos penales, desde la fase inicial de investigación previa al juicio hasta el cierre del proceso mediante sentencia u otra resolución. Las órdenes de entrega de datos de los abonados y de datos relativos al acceso pueden emitirse para cualquier infracción penal, mientras que las órdenes de entrega de datos de transacciones o de datos de contenido solo se podrán emitir para infracciones penales punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años, o para delitos específicos a que se refiere la propuesta y cuando exista un vínculo específico con herramientas electrónicas y delitos cubiertos por la Directiva sobre terrorismo (UE) 2017/541.

Dados los distintos niveles de intromisión de las medidas impuestas en relación con los datos solicitados, la propuesta establece una serie de condiciones y garantías entre las que se incluyen la obligación de obtener la validación previa de las órdenes por una autoridad judicial. La propuesta se aplica solo a los datos almacenados. La interceptación instantánea de las telecomunicaciones no está cubierta por la presente propuesta. La medida se limita a lo necesario y proporcionado para la finalidad del proceso penal de que se trate. También permite a los proveedores solicitar aclaraciones a las autoridades emisoras cuando sea necesario. Si los problemas no pueden resolverse y la autoridad emisora decide proceder a la ejecución, los proveedores de servicios podrán utilizar las mismas razones para oponerse a la ejecución por sus propias autoridades. Además, se ha establecido un procedimiento específico para los casos en que la obligación de facilitar datos entre en conflicto con una obligación derivada de la legislación de un país tercero.

La legislación de la UE protege los derechos de los sospechosos y los acusados en los procesos penales, y ya existen normas para la protección de los datos personales. No obstante, en el caso de las personas cuyos datos se solicitan, estas salvaguardias adicionales incluidas en la propuesta establecen derechos procesales para dichas personas dentro o fuera del proceso penal. Esto incluye la posibilidad de impugnar la legalidad, la necesidad o la proporcionalidad de la orden sin restringir los motivos de recurso de acuerdo con la legislación nacional. Los derechos con arreglo a la legislación del Estado de ejecución se respetan plenamente, asegurando que los privilegios e inmunidades que protegen los datos solicitados en el Estado miembro del proveedor de servicios se tengan en cuenta en el Estado emisor. Este es especialmente el caso cuando en el Estado de ejecución se contempla una protección mayor que la prevista en la legislación del Estado emisor.

Las órdenes en virtud del Reglamento propuesto son ejecutables de igual manera que las órdenes nacionales comparables en la jurisdicción en la que el proveedor de servicios recibe

la orden. El Reglamento establece que los Estados miembros deben fijar sanciones eficaces y proporcionadas.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

• Base jurídica

La base jurídica para la adopción de medidas en este ámbito es el artículo 82, apartado 1, del Tratado de Funcionamiento de la Unión Europea, que dispone que se podrán adoptar medidas con arreglo al procedimiento legislativo ordinario a fin de establecer normas y procedimientos para garantizar el reconocimiento en toda la Unión de las sentencias y resoluciones judiciales en todas sus formas. Podrán también adoptarse medidas para facilitar la cooperación entre las autoridades judiciales o equivalentes de los Estados miembros en el marco del proceso penal y de la ejecución de resoluciones.

Esta base jurídica se aplica a los mecanismos contemplados en el presente Reglamento. El artículo 82, apartado 1, garantiza el reconocimiento mutuo de las resoluciones judiciales por las que una autoridad judicial del Estado emisor se dirige a una persona jurídica de otro Estado miembro e incluso le impone obligaciones, sin intervención previa de una autoridad judicial en ese otro Estado miembro. La orden europea de entrega o la orden europea de conservación pueden dar lugar a la intervención de una autoridad judicial del Estado de ejecución cuando sea necesario para ejecutar la orden.

• Elección del instrumento

El artículo 82, apartado 1, del TFUE ofrece al legislador de la Unión la posibilidad de adoptar Reglamentos y Directivas.

Dado que la propuesta se refiere a procedimientos transfronterizos para los que se requieren normas uniformes, no es necesario dejar un margen a los Estados miembros para transponer dichas normas. Un Reglamento es directamente aplicable, aporta claridad y más seguridad jurídica y evita interpretaciones divergentes en los Estados miembros y otros problemas de transposición que han padecido las Decisiones marco relativas al reconocimiento mutuo de las sentencias y resoluciones judiciales. Además, un Reglamento permite imponer la misma obligación de manera uniforme en la Unión. Por estas razones, se considera que la forma más adecuada para este instrumento de reconocimiento mutuo es un Reglamento.

• Subsidiariedad

Teniendo en cuenta la dimensión transfronteriza de los problemas abordados, las medidas incluidas en la propuesta deben adoptarse a escala de la Unión con el fin de alcanzar los objetivos. Los delitos para los que existen pruebas electrónicas a menudo están vinculados a situaciones en las que la infraestructura en la que se almacena la prueba electrónica y el proveedor de servicios que gestiona la infraestructura se encuentran sometidos a un marco jurídico nacional diferente, en la Unión o fuera de ella, del marco jurídico nacional de la víctima y del autor del delito. En consecuencia, puede requerir mucho tiempo y ser muy difícil que el país competente acceda de forma efectiva a pruebas electrónicas transfronterizas si no existen normas mínimas comunes. En particular, si los Estados miembros actuasen por sí solos tendrían dificultades para abordar las siguientes cuestiones:

- la fragmentación de los marcos jurídicos en los Estados miembros, que se consideró un reto importante por los proveedores de servicios que deseen dar cumplimiento a solicitudes basadas en diferentes legislaciones nacionales;

- una mayor oportunidad de cooperación judicial sobre la base de la legislación vigente de la Unión, en particular a través de la orden europea de investigación.

Habida cuenta de la diversidad de enfoques jurídicos, el número de ámbitos políticos afectados (seguridad; derechos fundamentales, incluidos los derechos procesales y la protección de datos personales; y cuestiones económicas) y la amplia gama de partes interesadas, la legislación a escala de la Unión es el medio más adecuado para abordar los problemas detectados.

- **Proporcionalidad**

La propuesta establece normas en virtud de las cuales una autoridad competente de la Unión puede ordenar que un proveedor que ofrezca sus servicios en la Unión y que no esté establecido en el mismo Estado miembro, entregue o conserve pruebas electrónicas. Elementos clave de la propuesta, como el ámbito de aplicación material de la orden europea de entrega, las condiciones que garanticen la cortesía, el mecanismo de sanciones y el sistema de garantías y vías de recurso, limitan la propuesta a lo estrictamente necesario para alcanzar sus principales objetivos. En particular, la propuesta se limita a solicitudes de datos almacenados (no están contemplados los datos procedentes de la interceptación en tiempo real de las telecomunicaciones) y a las órdenes emitidas en un proceso penal respecto de una infracción penal específica objeto de investigación. Por tanto, no abarca la prevención de la delincuencia ni otros tipos de procesos o infracciones (tales como los procedimientos administrativos por vulneración de las normas jurídicas) y no exige a los proveedores que recopilen o almacenen sistemáticamente más datos de los que precisan para su actividad o para el cumplimiento de otros requisitos legales. Por otra parte, mientras que la orden de entrega de datos de los abonados y de datos relativos al acceso puede emitirse respecto de cualquier infracción penal, la orden de entrega de datos de transacciones o de datos de contenido puede emitirse únicamente respecto de infracciones punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años, o respecto de delitos relacionados con el ciberespacio o cometidos mediante la utilización del ciberespacio, o respecto de delitos de terrorismo. Por último, la propuesta aclara las normas de procedimiento y las salvaguardias aplicables al acceso transfronterizo a las pruebas electrónicas, pero no llega a armonizar las medidas nacionales. Se limita a lo necesario y proporcionado para abordar las necesidades de las autoridades policiales y judiciales en la era digital.

3. RESULTADOS DE LAS EVALUACIONES *A POSTERIORI*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- **Consultas con las partes interesadas**

Durante más de un año y medio, la Comisión consultó a todas las partes interesadas a fin de determinar los problemas y el camino a seguir. Esto se hizo a través de encuestas, desde una consulta pública abierta hasta encuestas específicas dirigidas a las autoridades públicas pertinentes. Se organizaron asimismo reuniones de grupos de expertos y reuniones bilaterales para discutir las posibles repercusiones de la legislación de la UE. También se recurrió a conferencias sobre el acceso transfronterizo a pruebas electrónicas para recabar opiniones sobre la iniciativa.

En general, los encuestados percibían que el aumento del uso de los servicios de información plantea un reto para las autoridades policiales y judiciales, ya que a menudo las autoridades pertinentes no están adecuadamente preparadas para la gestión en línea de pruebas. El largo

proceso de obtención de pruebas también se identifica como uno de los principales obstáculos. Otros asuntos clave que las autoridades públicas destacaron incluyen la falta de una cooperación fiable con los proveedores de servicios, la falta de transparencia y la inseguridad jurídica en cuanto a la jurisdicción correspondiente a las medidas de investigación. Se consideró que la cooperación transfronteriza directa entre las autoridades policiales y judiciales y los proveedores de servicios digitales añadiría valor en una investigación penal. Los proveedores de servicios y algunas organizaciones de la sociedad civil señalaron la necesidad de garantizar la seguridad jurídica a la hora de cooperar con las autoridades públicas y evitar conflictos de legislaciones. Con respecto a ciertas inquietudes sobre la forma en que una nueva legislación de la UE podría afectar a los derechos, las partes interesadas consideraron que deberían garantizarse salvaguardias específicas como condición necesaria para cualquier instrumento transfronterizo.

La información obtenida tras la evaluación de impacto inicial puso de manifiesto que las partes interesadas creían que abordar las deficiencias del actual sistema de asistencia judicial mutua sería más eficaz y mejoraría la seguridad jurídica. Algunas organizaciones de la sociedad civil se opusieron a una legislación a escala de la UE en materia de cooperación directa y prefirieron limitar la actuación de la UE a la mejora de los procedimientos de asistencia jurídica mutua. Esta idea se tendrá en cuenta como parte de las medidas prácticas aprobadas por el Consejo en junio de 2016.

A través de una encuesta específica dirigida a las autoridades públicas de los Estados miembros, también se puso de manifiesto que no existía un enfoque común sobre la obtención transfronteriza de pruebas electrónicas, ya que cada Estado miembro tiene sus propias prácticas internas. Los proveedores de servicios también reaccionan de forma distinta a las solicitudes de las autoridades policiales y judiciales extranjeras y el tiempo de respuesta varía en función del Estado miembro requirente. Esto crea inseguridad jurídica para todos los implicados.

En general, la consulta con las partes interesadas indicó que el marco jurídico actual es fragmentado y complejo. Ello puede dar lugar a retrasos durante la fase de ejecución y a la falta de una investigación y enjuiciamiento eficaces de los delitos que impliquen el acceso transfronterizo a pruebas electrónicas.

- **Evaluación de impacto**

El Comité de Control Reglamentario emitió un dictamen favorable acerca de la evaluación de impacto que acompaña a la presente propuesta[20] y presentó varias sugerencias de mejora[21]. A raíz de este dictamen, la evaluación de impacto fue modificada para seguir debatiendo las cuestiones de derechos fundamentales relacionadas con el intercambio transfronterizo de datos y, en particular, la relación entre las diferentes medidas que forman parte de la opción

[20] Documento de trabajo de los servicios de la Comisión - Evaluación de impacto que acompaña a la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal y a la propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, SWD(2018) 118.

[21] Comisión Europea - Dictamen del Comité de Control Reglamentario sobre la evaluación de impacto que acompaña a la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal y a la propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, SEC(2018) 199.

preferida. La evaluación también se modificó para reflejar mejor los puntos de vista de las partes interesadas y los Estados miembros y la manera en que se han tenido en cuenta. Por otra parte, se revisó el contexto político para incluir más referencias a diversos aspectos, por ejemplo, los debates en los grupos de expertos que contribuyeron a dar forma a la iniciativa. La complementariedad entre diferentes medidas (en particular, la Directiva sobre la orden europea de investigación, las negociaciones de un protocolo adicional al Convenio de Budapest y la revisión conjunta del Acuerdo de asistencia judicial mutua UE-EE.UU.) se aclaró en términos de alcance, calendario y profundidad, y el escenario de base se revisó para reflejar mejor la evolución que probablemente se produzca con independencia de la adopción de las medidas propuestas. Por último, se añadieron diagramas para describir mejor el flujo de trabajo del intercambio de datos.

Se consideraron cuatro opciones estratégicas además de la hipótesis de referencia (opción O): una serie de medidas prácticas destinadas a mejorar los procedimientos de cooperación judicial y la cooperación directa entre autoridades públicas y proveedores de servicios (opción A: no legislativa); una opción que combina las medidas prácticas de la opción A con soluciones internacionales a nivel bilateral o multilateral (opción B: legislativa); una opción que incluye las medidas anteriores contenidas en la opción B, con una orden europea de entrega, y una medida destinada a mejorar el acceso a las bases de datos que informan sobre los abonados cuando se buscan dichos datos, como el nombre de dominio WHOIS (opción C: legislativa); una opción que incluye todas las medidas anteriores incluidas en la opción C con legislación sobre el acceso directo a datos almacenados a distancia (opción D: legislativa)[22].

Si no se adopta ninguna medida (opción O), un número creciente de solicitudes empeorará la situación. Todas las demás opciones contribuyen a alcanzar los objetivos de la iniciativa, pero en grados diferentes. La opción A mejoraría la eficiencia de los procesos actuales, por ejemplo mediante la mejora de la calidad de las solicitudes, pero el margen de mejora se vería limitado por las deficiencias estructurales del sistema actual.

La opción B podría dar lugar a más mejoras al prever soluciones aceptadas a nivel internacional, pero el resultado de estas soluciones internacionales dependería, en gran medida, de Estados terceros. Por consiguiente, las soluciones son inciertas y es poco probable que sean tan eficaces y ofrezcan tantas garantías como una solución a escala de la Unión.

La opción C supondría un claro valor añadido en comparación con las opciones anteriores, al prever también un instrumento en el seno de la UE en materia de cooperación directa con los proveedores de servicios, que resolvería la mayoría de los problemas identificados cuando exista un proveedor de servicios que posea los datos en cuestión.

La opción D es el paquete de soluciones más completo. Además de las medidas anteriores, se trata de una medida legislativa sobre acceso directo para situaciones en las que no es necesaria la participación de un proveedor de servicios.

La presente iniciativa legislativa que propone la Comisión se basa en las conclusiones de la evaluación de impacto. Esta legislación se complementará con las medidas concretas descritas en la evaluación de impacto y con trabajos posteriores para elaborar un protocolo adicional al

[22] Para más detalles, véase la evaluación de impacto que acompaña a la propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal y a la propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, SWD(2018) 118.

Convenio de Budapest. Sobre la base de su propuesta legislativa, la Comisión también debatirá con Estados Unidos y otros países terceros la posibilidad de futuros acuerdos bilaterales o multilaterales sobre el acceso transfronterizo a pruebas electrónicas con las salvaguardias correspondientes. En el caso de las medidas sobre acceso directo y acceso a las bases de datos, que forman parte de la opción D, la Comisión no propone por el momento legislación alguna, pero seguirá reflexionando sobre la mejor forma de seguir avanzando en estas dos cuestiones.

Se espera que la iniciativa permita unas investigaciones y enjuiciamientos más eficaces y eficientes, mejorando al mismo tiempo la transparencia y la rendición de cuentas y garantizando el respeto de los derechos fundamentales. También se espera fomentar la confianza en el mercado único digital, mejorando la seguridad y la reducción de la percepción de impunidad para los delitos cometidos en dispositivos interconectados o a través de los mismos.

Para las autoridades públicas, se espera que la iniciativa genere costes de aplicación iniciales, que a largo plazo se verían compensados por ahorros en los gastos corrientes. Las autoridades nacionales tendrían que adaptarse a los nuevos procedimientos y recibir formación. Sin embargo, posteriormente se beneficiarían de la simplificación y la centralización, así como del marco jurídico claro que regula las solicitudes de acceso a los datos, ya que ello generaría mejoras de eficiencia. Del mismo modo, dado que la opción preferida reduciría la presión sobre los canales de cooperación judicial, los países que reciban peticiones deberían observar una reducción del número de peticiones que deben tramitar.

Los proveedores de servicios tendrían que adaptarse a un nuevo marco legislativo mediante la instauración de (nuevos) procedimientos y la formación de su personal. Por otra parte, un marco armonizado podría reducir la carga que pesa actualmente sobre los proveedores para responder a solicitudes de datos distintos a los datos de contenido, pues deben evaluarlas con arreglo a las distintas normativas de todos los Estados miembros. La seguridad jurídica y la normalización de los procedimientos deberían repercutir también positivamente sobre las pymes, ya que se aliviaría la carga administrativa y se favorecería la competitividad. En general, también se espera que la iniciativa genere ahorros para ellas.

- **Derechos fundamentales**

La propuesta podría afectar a una serie de derechos fundamentales:

- derechos de la persona a cuyos datos se accede: derecho a la protección de los datos personales, derecho al respeto de la vida privada y familiar, derecho a la libertad de expresión, derecho de defensa, y derecho a la tutela judicial efectiva y a un juicio justo;
- derechos del proveedor de servicios: derecho a la libertad de empresa y derecho a la tutela judicial efectiva;
- derechos de los ciudadanos: derecho a la libertad y a la seguridad.

Teniendo en cuenta el acervo pertinente en materia de protección de datos, se han incluido salvaguardias importantes y suficientes en la propuesta de Reglamento a fin de garantizar la protección de los derechos de estas personas.

Dado que las órdenes solo pueden emitirse en procesos penales y si existen situaciones nacionales comparables, tanto durante las fases previas como durante la celebración del juicio, todas las garantías procesales de Derecho penal son aplicables. Esto incluye, en

particular, el derecho a un proceso equitativo consagrado en el artículo 6 del CEDH y en los artículos 47 y 48 de la Carta de los Derechos Fundamentales. También incluye la legislación pertinente a escala de la UE sobre derechos procesales en los procesos penales: la Directiva 2010/64/UE relativa al derecho a interpretación y a traducción en los procesos penales; la Directiva 2012/13/UE relativa al derecho a la información en los procesos penales; la Directiva 2013/48/UE sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad; la Directiva 2016/343 por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio; la Directiva 2016/800 relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales; y la Directiva 2016/1919 relativa a la asistencia jurídica gratuita a los sospechosos y acusados en los procesos penales y a las personas buscadas en virtud de un procedimiento de orden europea de detención.

Más concretamente, la intervención previa de la autoridad judicial cuando se emite la orden garantiza que se ha verificado la legalidad de la medida, así como su necesidad y proporcionalidad con respecto al asunto en cuestión. Esto también garantiza que la orden no lesiona indebidamente los derechos fundamentales, en particular el respeto de principios jurídicos como el secreto profesional de los abogados. La autoridad emisora está obligada a velar, en cada caso concreto, porque la medida sea necesaria y proporcionada, teniendo en cuenta la gravedad de la infracción objeto de investigación. La propuesta incluye asimismo umbrales para los datos de transacciones y de contenido, garantizando que la orden europea de entrega solo podrá utilizarse para formas más graves de delitos, en lo que respecta a esos datos.

También se aborda explícitamente el derecho a una tutela judicial efectiva para las personas cuyos datos se solicitan. Los privilegios e inmunidades de determinadas profesiones, como la de abogado, así como los intereses fundamentales de seguridad y defensa nacionales del Estado destinatario, también deberán tenerse en cuenta durante el juicio en el Estado emisor. La revisión por una autoridad judicial funciona como una garantía adicional a este respecto.

Puesto que la orden es una medida vinculante, afecta también a los derechos de los proveedores de servicios, en particular, la libertad de empresa. La propuesta incluye el derecho del proveedor de servicios a presentar determinadas alegaciones en el Estado miembro emisor, por ejemplo en caso de que la orden no haya sido emitida o validada por una autoridad judicial. En caso de que la orden se transmita para su ejecución al Estado de ejecución, la autoridad de ejecución podrá decidir, después de consultar a la autoridad emisora, no reconocer o ejecutar la orden si, tras su recepción, considera que se aplica alguno de los motivos limitados de oposición. Además, en caso de que se incoe el procedimiento de ejecución, el propio destinatario podrá oponerse a la orden ante la autoridad encargada de la ejecución sobre la base de esos motivos limitados. Esto incluye, por ejemplo, los casos en que es evidente que la orden no ha sido emitida o validada por una autoridad competente, o los casos en que el cumplimiento de la orden violaría manifiestamente la Carta o sería manifiestamente abusivo. Esto no excluye el derecho del destinatario a un recurso judicial efectivo contra una decisión por la que se impone una sanción.

Un problema potencial relacionado con las medidas de la UE en este ámbito es la posibilidad de que pudieran dar lugar a que países terceros estableciesen obligaciones recíprocas para los proveedores de servicios de la UE que no fueran compatibles con los derechos fundamentales de la UE, en particular el alto nivel de protección de los datos garantizado por el acervo de la

UE. La propuesta aborda esta situación de dos maneras: en primer lugar, estableciendo una medida que contiene garantías sólidas y referencias expresas a las condiciones y garantías ya inherentes al acervo de la UE, sirviendo así de modelo para la legislación extranjera; y, en segundo lugar, mediante la inclusión de una cláusula sobre «conflictos de obligaciones» que permite a los proveedores determinar y plantear la existencia de obligaciones contradictorias a las que deben responder, lo que pone en marcha un control judicial. Esta cláusula tiene por objeto garantizar el respeto de las disposiciones generales de bloqueo, como, por ejemplo, la ley estadounidense sobre la privacidad de las comunicaciones electrónicas (*U. S. Electronic Communications Privacy Act, ECPA*), que prohíbe la divulgación de datos de contenido en su ámbito geográfico, excepto en circunstancias determinadas, así como el respeto de leyes que generalmente no prohíben la revelación, aunque pueden hacerlo en casos específicos. Actualmente, en los casos relativos a la ECPA, el acceso a los datos de contenido podrá impedirse en determinadas situaciones, por lo que la asistencia judicial mutua debería seguir siendo el principal instrumento para acceder a ellos. Sin embargo, con las modificaciones introducidas mediante la adopción de la Ley estadounidense CLOUD (*U.S. Cloud Act*) [23], la disposición de bloqueo podría anularse si la UE llegara a un acuerdo con Estados Unidos. Otros acuerdos internacionales adicionales con socios clave podrían reducir todavía más las situaciones conflictivas.

En vista de lo anterior, las medidas previstas en la propuesta son compatibles con los derechos fundamentales.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta legislativa de Reglamento no tiene repercusiones en el presupuesto de la Unión.

5. OTROS ELEMENTOS

- **Planes de ejecución y modalidades de seguimiento, evaluación e información**

El Reglamento es directamente aplicable en la Unión. Será directamente aplicado por los profesionales, sin necesidad de modificar los ordenamientos jurídicos internos.

El Reglamento será evaluado y la Comisión presentará un informe al Parlamento Europeo y al Consejo a más tardar cinco años después de su entrada en vigor. Sobre la base de las conclusiones del informe, y en particular de si el Reglamento deja lagunas que serían importantes en la práctica, y teniendo en cuenta los avances tecnológicos, la Comisión evaluará la necesidad de ampliar el ámbito de aplicación del Reglamento. En caso necesario, la Comisión presentará propuestas para adaptar el presente Reglamento. Los Estados miembros facilitarán a la Comisión la información necesaria para la preparación del informe y recopilarán los datos necesarios para realizar un control anual del Reglamento.

Si resulta necesario, la Comisión elaborará orientaciones para que los proveedores de servicios puedan cumplir las obligaciones derivadas del Reglamento.

- **Explicación detallada de las disposiciones específicas de la propuesta**

[23] El 23 de marzo de 2018, Estados Unidos adoptó la Clarifying Lawful Overseas Use of Data (CLOUD) Act (Ley de clarificación de la utilización lícita de los datos en el extranjero (CLOUD Act), que puede consultarse aquí.

	REGLAMENTO	
	Artículo	**Considerandos**
I. Objeto, definiciones y ámbito de aplicación	1. Objeto	1-15
	2. Definiciones	16-23
	3. Ámbito de aplicación	24-27
II. Orden europea de entrega, orden europea de conservación, certificados, representante legal	4. Autoridad emisora	30
	5. Condiciones para la emisión de una orden europea de entrega	31-35, 28-29
	6. Condiciones para la emisión de una orden europea de conservación	36
	7. Destinatario de la orden europea de entrega y de la orden europea de conservación	37
	8. Certificado de orden europea de entrega y certificado de orden europea de conservación	38-39
	9. Ejecución del EPOC	40-41
	10. Ejecución del EPOC-PR	42
	11. Confidencialidad e información al usuario	43
	12. Reembolso de gastos	Ninguno
III. Sanciones y ejecución	13. Sanciones	Ninguno
	14. Procedimiento de ejecución	44-45, 55
IV. Vías de recurso	15. y 16. Procedimiento de recurso en caso de obligaciones contradictorias derivadas del Derecho de un país tercero	47-53
	17. Vías de recurso efectivas	54
	18. Respeto de los privilegios e inmunidades en virtud de la legislación del Estado de ejecución	35
V. Disposiciones finales	19. Seguimiento y presentación de informes	58
	20. Modificaciones de los certificados y formularios	59-60
	21. Ejercicio de la delegación	60
	22. Notificaciones	Ninguno
	23. Relación con las órdenes europeas de investigación	61
	24. Evaluación	62
	25. Entrada en vigor	Ninguno

Capítulo 1: Objeto, definiciones y ámbito de aplicación

Artículo 1: Objeto

Este artículo establece el alcance general y el objetivo de la propuesta, que es establecer normas en virtud de las cuales una autoridad judicial competente de la Unión Europea podrá ordenar a un proveedor que ofrezca servicios en la Unión que entregue o conserve pruebas electrónicas mediante una orden europea de entrega o de conservación. Estos instrumentos solo pueden utilizarse en situaciones transfronterizas, es decir, en situaciones en las que el proveedor de servicios esté establecido o representado en otro Estado miembro.

El presente Reglamento ofrecerá instrumentos adicionales a las autoridades de investigación para que obtengan pruebas electrónicas, sin limitar las competencias ya previstas por la legislación nacional para obligar a los proveedores de servicios establecidos o representados en su territorio a cumplir las disposiciones aplicables. Si el proveedor de servicios está establecido o representado en el mismo Estado miembro, las autoridades de dicho Estado miembro utilizarán por tanto las medidas nacionales para obligar al proveedor de servicios a cumplir las disposiciones aplicables.

Los datos solicitados a través de una orden europea de entrega deberán comunicarse directamente a las autoridades sin intervención de las autoridades del Estado miembro en el que el proveedor de servicios esté establecido o representado. El Reglamento también descarta la ubicación de los datos como factor de vinculación determinante, ya que el almacenamiento de datos normalmente no da lugar a ningún control por parte del Estado en cuyo territorio se almacenan. El almacenamiento es determinado únicamente por el proveedor en la mayoría de los casos y sobre la base de consideraciones comerciales[24].

Por otra parte, el Reglamento también es aplicable si los proveedores de servicios no están establecidos o representados en la Unión, pero ofrecen servicios en la Unión. Esto se refleja en el artículo 3, apartado 1.

Cuando la propuesta se refiere a un proveedor de servicios establecido o representado en un Estado miembro por un único representante legal designado, su mera designación no crea un establecimiento del proveedor de servicios a efectos del presente Reglamento.

El artículo 1, apartado 2, recuerda que el presente Reglamento no podrá tener por efecto modificar la obligación de respetar los derechos fundamentales y los principios jurídicos consagrados en el artículo 6 del Tratado de la Unión Europea.

Artículo 2: Definiciones

Este artículo recoge las definiciones que se aplican en todo el instrumento.

Los siguientes tipos de proveedores de servicios entran en el ámbito de aplicación del Reglamento: los proveedores de servicios de comunicaciones electrónicas, los proveedores de servicios de la sociedad de la información para que los que el almacenamiento de datos es un componente determinante del servicio prestado al usuario, incluidas las redes sociales (en la medida en que no se consideren servicios de comunicaciones electrónicas), los mercados en línea que facilitan transacciones entre sus usuarios (consumidores o empresas) y otros proveedores de servicios de alojamiento de datos y proveedores de servicios de asignación de nombres y números en internet.

El ámbito de aplicación del Reglamento incluye a los proveedores de servicios de comunicaciones electrónicas, según se define [en la Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas]. Los servicios tradicionales de telecomunicaciones, los consumidores y las empresas recurren cada vez más a los nuevos servicios basados en internet que permiten comunicaciones interpersonales, tales como los de voz sobre IP, de mensajería instantánea y de correo electrónico, en lugar de los servicios de comunicación tradicionales. Estos servicios, junto con redes sociales como Twitter y

[24] La evaluación de impacto contiene más explicaciones.

Facebook, que permiten a los usuarios compartir contenidos, deben por tanto estar cubiertos por la presente propuesta.

En muchos casos, los datos ya no se almacenan en el dispositivo del usuario, sino que están disponibles a través de una infraestructura basada en la nube que permite, en principio, acceder a ellos desde cualquier lugar. Los proveedores de servicios no necesitan estar establecidos o tener servidores en todas las jurisdicciones, sino utilizar una administración centralizada y sistemas descentralizados para almacenar los datos y prestar sus servicios. Esta solución les permite optimizar el equilibrado de carga y acortar el tiempo de respuesta a las solicitudes de datos de los usuarios. Generalmente, las redes de distribución de contenidos se implantan para agilizar la distribución de contenidos, copiándolos en varios servidores distribuidos por todo el mundo. Esto permite a las empresas enviar el contenido desde el servidor que esté más próximo al usuario o que pueda canalizar la comunicación a través de una red menos congestionada. Para tener en cuenta esta evolución, la definición abarca los servicios de almacenamiento en la nube y otros servicios de alojamiento que aportan una gran variedad de recursos informáticos, tales como redes, servidores u otras infraestructuras, almacenamiento, aplicaciones y servicios que permiten almacenar datos para fines diferentes. El instrumento también se aplica a los mercados digitales que permiten a los consumidores o a las empresas realizar transacciones a través de contratos de venta o de servicios en línea. Estas transacciones se realizan bien en el sitio web del mercado en línea o en una página web del comerciante que utilice servicios informáticos prestados por el mercado en línea. Por consiguiente, este mercado es el que está en posesión de las pruebas electrónicas que pueden ser necesarias en el marco de un proceso penal.

Los servicios para los que el almacenamiento de datos no es un componente determinante no están cubiertos por la presente propuesta. Aunque la mayoría de los servicios ofrecidos por los proveedores implican algún tipo de almacenamiento de datos, especialmente cuando se trata de servicios en línea prestados a distancia, cabe distinguir los servicios para los que el almacenamiento de datos no es una característica principal, sino meramente accesoria, como los servicios jurídicos, de arquitectura, de ingeniería y de contabilidad prestados en línea, a distancia.

Los datos que obran en poder de los proveedores de servicios de infraestructuras de internet, como los registros y registradores de nombres de dominio y los proveedores de servicios de privacidad y representación, o los registros regionales de direcciones de protocolo de internet, pueden ser relevantes para los procesos penales, ya que pueden ofrecer indicios que permitan la identificación de una persona o entidad implicada en actividades delictivas.

Las categorías de datos que podrán obtener las autoridades competentes con una orden europea de entrega incluyen los datos de los abonados, los datos relativos al acceso, los datos de transacciones (estas tres categorías de datos se denominan generalmente «datos no relativos al contenido») y los datos de contenido almacenados. Esta distinción, aparte de los datos relativos al acceso, existe en los ordenamientos jurídicos de numerosos Estados miembros y también en los de países terceros.

Todas las categorías contienen datos personales, y por tanto están cubiertas por las salvaguardias previstas en el acervo de la UE en materia de protección de datos. La intensidad del impacto en los derechos fundamentales varía entre las categorías, en particular entre los datos de los abonados, por una parte, y los datos de transacciones y de contenido, por otra. Es esencial que todas estas categorías estén cubiertas por el instrumento, pues los datos de los abonados y los datos relativos al acceso a menudo son el punto de partida para obtener pistas

en una investigación sobre la identidad de un sospechoso, aunque los datos de transacciones y de contenido pueden ser más relevantes como material probatorio. A causa de los distintos niveles de injerencia en los derechos fundamentales, está justificado poner condiciones diferentes a los datos de los abonados, por una parte, y a los datos de transacciones y de contenido, por otra, tal como figura en varias disposiciones del Reglamento.

Procede destacar los datos relativos al acceso como una categoría específica de datos utilizada en el presente Reglamento. Los datos relativos al acceso, según se definen en el Reglamento, se solicitan para el mismo objetivo que los datos de los abonados, es decir, identificar al usuario, y el grado de injerencia en los derechos fundamentales es similar. Por tanto, deben estar sujetos a las mismas condiciones que los datos de los abonados. La presente propuesta introduce así una nueva categoría de datos, que debe tratarse igual que los datos de los abonados, si persiguen el mismo objetivo.

El artículo 2 define los Estados miembros y autoridades que pueden participar en el proceso. El artículo 4 contiene una definición de la autoridad emisora.

Los casos urgentes son situaciones excepcionales que requieren una reacción oportuna de los proveedores de servicios y a las que se aplican condiciones especiales. Por tanto, se definen por separado en este artículo.

Artículo 3: Ámbito de aplicación

Este artículo establece el ámbito de aplicación de la propuesta. El Reglamento se aplica a todos los proveedores que prestan servicios en la Unión, incluidos los proveedores que no están establecidos en la Unión. La oferta activa de servicios en la Unión, con todas sus ventajas, justifica que estos proveedores también estén sujetos al Reglamento, y crea unas condiciones de competencia equitativas entre los participantes en los mismos mercados. Por otra parte, la no inclusión de dichos proveedores de servicios crearía una laguna jurídica y facilitaría a los delincuentes eludir el ámbito de aplicación del Reglamento.

A fin de determinar si se ofrecen servicios, las autoridades deberán evaluar si el proveedor de servicios permite que personas físicas o jurídicas de uno o varios Estados miembros utilicen sus servicios. No obstante, la mera accesibilidad del servicio (que también puede resultar de la accesibilidad del sitio web del proveedor de servicios, de un intermediario, de una dirección de correo electrónico y de otros datos de contacto) no debe ser condición suficiente para la aplicación del presente Reglamento. Por consiguiente, es necesaria una vinculación significativa a dichos Estados miembros para establecer una relación suficiente entre el proveedor y el territorio en el que presta sus servicios. Tal vinculación significativa existe cuando un proveedor de servicios tiene un establecimiento en uno o más Estados miembros. A falta de un establecimiento en la Unión, el criterio de vinculación significativa a la Unión se evaluará sobre la base de la existencia de un número significativo de usuarios en uno o más Estados miembros, o en la orientación de las actividades hacia uno o más Estados miembros. Esta orientación puede determinarse en virtud de todas las circunstancias pertinentes, incluidos factores como el uso de una lengua o una moneda utilizada generalmente en un Estado miembro. La orientación de las actividades hacia un Estado miembro también puede derivarse de la disponibilidad de una aplicación móvil en la tienda de aplicaciones nacional pertinente, de la divulgación de publicidad local en la lengua utilizada en un Estado miembro, de la utilización de cualquier información procedente de personas localizadas en los Estados miembros en el marco de sus actividades, o de la gestión de las relaciones con los clientes, por ejemplo a través de la prestación de servicios a los clientes en la lengua generalmente

utilizada en un Estado miembro. También se supone un vínculo sustancial cuando un proveedor de servicios dirige su actividad hacia uno o varios Estados miembros con arreglo a lo establecido en el artículo 17, apartado 1, letra c), del Reglamento n.º 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

La orden europea de entrega y la orden europea de conservación son medidas de investigación que solo podrán emitirse en investigaciones o procesos penales para infracciones penales específicas. La vinculación con una investigación específica distingue estas órdenes de las medidas preventivas o de las obligaciones de conservación de datos establecidas por ley, y garantiza la aplicación de los derechos procesales aplicables a los procesos penales. La competencia para iniciar investigaciones respecto de una infracción específica constituye, por tanto, una condición necesaria para la aplicación del Reglamento.

Como requisito adicional, los datos solicitados deberán guardar relación con los servicios prestados por el proveedor de servicios en la Unión.

Capítulo 2: Orden europea de entrega, orden europea de conservación y certificados

Artículo 4: Autoridad emisora

Cuando se emita una orden europea de entrega o de conservación, siempre deberá intervenir en el proceso una autoridad judicial que actúe en calidad de autoridad emisora o de validación. En el caso de las órdenes de entrega de datos de transacciones y datos de contenido, se requiere la intervención de un juez o un tribunal. Para la obtención de datos de los abonados y de datos relativos al acceso, los fiscales también podrán emitir órdenes.

Artículo 5: Condiciones para la emisión de una orden europea de entrega

El artículo 5 establece las condiciones para la emisión de una orden europea de entrega, condiciones que deberán ser evaluadas por la autoridad judicial emisora.

La orden europea de entrega solo podrá emitirse si es necesaria y proporcionada en el caso de autos. Por otra parte, la orden solo podrá emitirse si existe una medida similar en una situación nacional comparable en el Estado emisor.

Las órdenes europeas de entrega de datos de los abonados o de datos relativos al acceso podrán ser emitidas para cualquier infracción penal. Los datos de transacciones y los datos de contenido deberán estar sujetos a unos requisitos más estrictos, con objeto de reflejar su naturaleza más sensible y, por tanto, el mayor grado de intrusión de las órdenes referentes a dichos datos, en comparación con los datos de los abonados y los datos relativos al acceso. Así pues, las órdenes solo podrán emitirse respecto de infracciones penales punibles con una pena máxima de privación de libertad de al menos tres años. La fijación de un umbral basado en una pena de privación de libertad de duración máxima permite un enfoque más proporcionado, junto con varias otras condiciones previas y posteriores y salvaguardias destinadas a garantizar el respeto de la proporcionalidad y los derechos de las personas afectadas.

Al mismo tiempo, el umbral no debe comprometer la eficacia del instrumento y su utilización por parte de los profesionales. Los Estados miembros aplicarán penas de duración máxima de conformidad con sus sistemas nacionales. Los códigos penales nacionales varían y no están armonizados. Este es el caso de las infracciones penales y de las sanciones aplicables. Los

códigos procesales nacionales también difieren en relación con los umbrales para la obtención de datos de transacciones y datos de contenido: algunos Estados miembros no establecen ningún umbral específico, mientras que otros prevén una lista de infracciones penales. Un umbral de tres años restringe el ámbito de aplicación del instrumento a los delitos más graves, sin limitar excesivamente las posibilidades de su uso por los profesionales. Este umbral excluye del ámbito de aplicación una amplia gama de delitos, dependiendo del código penal del Estado miembro (por ejemplo, en algunos Estados miembros, la participación en actividades de grupos delictivos organizados y el secuestro, pero también hurtos, fraudes y agresiones, para los que el uso de una orden de entrega transfronteriza para obtener datos más sensibles puede considerarse desproporcionado). Por otra parte, un umbral de tres años incluye delitos que requieren un enfoque más eficaz, como es el caso de la participación en una organización delictiva, la financiación de grupos terroristas, el apoyo o la publicidad de una organización delictiva, la formación para cometer delitos de terrorismo, algunos delitos cometidos con intención terrorista y la preparación de una infracción penal con fines terroristas o la preparación de la toma de rehenes, que de otro modo quedarían excluidos si se aplicase un umbral más elevado, dependiendo de la legislación aplicable del Estado miembro. Este umbral se ha elegido para garantizar un equilibrio entre la eficacia de las investigaciones penales y la protección de los derechos y de la proporcionalidad en todos los Estados miembros. Un umbral también tiene la ventaja de ser fácilmente aplicable en la práctica.

Por otra parte, las órdenes de entrega de datos de transacciones o de datos de contenido también podrán emitirse para infracciones específicas armonizadas enumeradas en la disposición, para las que las pruebas normalmente estarán disponibles, en su mayoría, únicamente en formato electrónico. Ello justifica la aplicación del Reglamento también en aquellos casos en que las infracciones penales son punibles con una pena privativa de libertad de duración máxima por debajo del umbral indicado anteriormente; en caso contrario, esas infracciones no podrían investigarse adecuadamente, lo que podría dar lugar a impunidad. Las infracciones son disposiciones específicas de los siguientes actos legislativos: i) Decisión marco 2001/413/JAI del Consejo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; ii) Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo; y iii) Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Las órdenes también podrán emitirse para las infracciones penales enumeradas en la Directiva (UE) 2017/541 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. Algunas de estas infracciones tienen umbrales máximos de al menos un año, otras de dos años, pero ninguna de las infracciones tiene umbrales máximos inferiores a un año.

El artículo establece también la información obligatoria que debe figurar en la orden europea de entrega, con el fin de permitir que el proveedor de servicios identifique y entregue los datos solicitados. La justificación de la necesidad y la proporcionalidad de esta medida también forma parte de la orden europea de entrega.

La orden europea de entrega se ejecuta mediante la emisión de un certificado de orden europea de entrega (EPOC, por sus siglas en inglés) (véase el artículo 8), que se traduce y envía al proveedor de servicios. El certificado contiene la misma información obligatoria que consta en la orden, salvo la justificación de la necesidad y la proporcionalidad de la medida u otros datos del caso.

En los casos en que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa, normalmente en el caso de servicios de alojamiento o de programas informáticos, la propia empresa deberá ser la principal destinataria de una solicitud de las autoridades de investigación. En caso de que la empresa no sea un proveedor de servicios cubierto por el ámbito de aplicación del presente Reglamento, puede ser necesario recurrir a una orden europea de investigación o una petición de asistencia judicial. Al proveedor de servicios solo podrá notificársele una orden europea de entrega si no procede dirigirse a la empresa, en particular cuando ello pudiera poner en peligro la investigación, por ejemplo cuando la propia empresa esté siendo investigada.

Antes de emitir una orden europea de entrega, la autoridad emisora deberá tener en cuenta asimismo los privilegios e inmunidades que puedan estar previstos en la legislación del Estado miembro del proveedor de servicios o cualquier impacto en los intereses fundamentales de dicho Estado miembro tales como la seguridad y defensa nacionales. Esta disposición tiene por objeto garantizar que los privilegios e inmunidades que protegen los datos solicitados en el Estado miembro del proveedor de servicios se tengan en cuenta en el Estado emisor, en particular cuando prevean una mayor protección que la legislación del Estado emisor.

Artículo 6: Condiciones para la emisión de una orden europea de conservación

Una orden europea de conservación está sujeta a condiciones similares a las de la orden europea de entrega, y podrá emitirse para cualquier infracción penal, de conformidad con las demás condiciones establecidas en el artículo 6. Su objetivo es evitar la retirada, supresión o alteración de datos pertinentes en situaciones en las que la entrega de estos datos pueda llevar más tiempo, por ejemplo porque se utilicen canales de cooperación judicial. Teniendo en cuenta, por ejemplo, que en general la orden europea de investigación puede emitirse para cualquier infracción penal sin la imposición de umbrales, la orden europea de conservación tampoco estará sujeta a limitación. En caso contrario, este instrumento no sería eficaz. A fin de permitir que las autoridades de investigación actúen con rapidez y, dado que la correspondiente solicitud de entrega de datos será una solicitud posterior en que se analizarán nuevamente todas las condiciones, las órdenes europeas de conservación también podrán ser emitidas o validadas por un fiscal.

Artículo 7: Destinatario de la orden europea de entrega y de la orden europea de conservación

Las órdenes europeas de entrega y las órdenes europeas de conservación deberán remitirse directamente al representante legal designado por el proveedor de servicios a efectos de recabar pruebas para procesos penales, de conformidad con la Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales. La transmisión se hará en forma de un certificado de orden europea de entrega (EPOC) o de un certificado de orden europea de conservación (EPOC-PR), tal como se contempla en el artículo 8. Dicho representante legal será responsable de su recepción y ejecución completa a su debido tiempo, lo que permite a los proveedores decidir cómo organizarse para entregar los datos solicitados por las autoridades de los Estados miembros.

Si no se ha designado un representante legal, las órdenes podrán remitirse a cualquier establecimiento del proveedor en la Unión. Esta opción alternativa sirve para garantizar la eficacia del sistema en caso de que el proveedor de servicios (todavía) no haya designado un

representante específico, por ejemplo cuando no exista la obligación de designar un representante legal de conformidad con la Directiva, porque los proveedores de servicios estén establecidos y operen en un solo Estado miembro, o en caso de que todavía no haya entrado en vigor la obligación de designar un representante legal, antes de la expiración del plazo de transposición de la Directiva.

En caso de incumplimiento por el representante legal, existen dos situaciones en las que la autoridad emisora podrá dirigirse a cualquier establecimiento del proveedor en la Unión: en situaciones de urgencia, tal como se definen en el artículo 9, apartado 2, y en los casos en que el representante legal no cumpla las obligaciones que le incumben en virtud de los artículos 9 y 10, y en que la autoridad emisora considere que existen claros riesgos de pérdida de datos.

Artículo 8: Certificado de orden europea de entrega y certificado de orden europea de conservación

El EPOC y el EPOC-PR sirven para transmitir las órdenes al destinatario definido en el artículo 7. Los modelos de certificados figuran en los anexos I y II del Reglamento, y deben traducirse a una de las lenguas oficiales del Estado miembro en que esté establecido el destinatario. El proveedor de servicios podrá declarar que las órdenes se aceptarán también en otras lenguas oficiales de la Unión. Los certificados tienen por objeto facilitar toda la información necesaria al beneficiario en un formato normalizado, a fin de minimizar errores, permitir la fácil identificación de los datos, y evitar, en la medida de lo posible, el texto libre, reduciendo por tanto los gastos de traducción. No deberán incluirse en el certificado la justificación completa de la necesidad y la proporcionalidad de la medida, ni precisiones adicionales sobre el caso, a fin de no poner en peligro las investigaciones. Esta información solo deberá incluirse en la orden, de modo que, posteriormente, el sospechoso pueda impugnarla durante el proceso penal.

Algunos proveedores de servicios ya han creado plataformas para la presentación de solicitudes de las autoridades competentes. El Reglamento no deberá impedir el uso de estas plataformas, ya que ofrece muchas ventajas, como la posibilidad de una autenticación fácil y una transmisión segura de los datos. Sin embargo, estas plataformas deberán permitir la presentación del EPOC y el EPOC-PR en el formato establecido en los anexos I y II, sin solicitar datos adicionales relativos a la orden.

Las plataformas creadas por los Estados miembros o por los organismos de la Unión también pueden proporcionar medios seguros de transmisión y facilitar la autenticación de las órdenes y la recogida de datos. Debe considerarse una posible ampliación de las plataformas eCodex y SIRIUS para incluir una conexión segura a los proveedores de servicios a efectos de la notificación del EPOC y del EPOC-PR, y en su caso, para la transmisión de las respuestas de los proveedores de servicios.

Artículo 9: Ejecución del EPOC

El artículo 9 obliga a los destinatarios a responder a los EPOC e introduce plazos obligatorios. El plazo normal es de 10 días, aunque las autoridades podrán acortarlo cuando esté justificado. Por otra parte, en situaciones de urgencia, definidas como situaciones en las que exista una amenaza inminente para la vida o la integridad física de una persona o para una infraestructura crítica, el plazo será de 6 horas.

La disposición también garantiza la posibilidad de diálogo entre el destinatario y la autoridad emisora. Si el EPOC está incompleto, es manifiestamente incorrecto o no contiene

información suficiente para permitir su ejecución por el proveedor de servicios, el destinatario deberá ponerse en contacto con la autoridad emisora y solicitar aclaraciones, utilizando el formulario que figura en el anexo III. También informará a la autoridad emisora en los casos en que no pueda facilitar los datos debido a fuerza mayor o imposibilidad de hecho, por ejemplo si la persona cuyos datos se solicitan no es un cliente del servicio, o si (por ejemplo, debido a otras obligaciones de confidencialidad), los datos han sido legítimamente suprimidos por el proveedor de servicios antes de que este (o su representante legal) recibieran la orden. La autoridad emisora deberá tener conocimiento de estas circunstancias para reaccionar con rapidez, para quizás tratar de obtener las pruebas electrónicas de otro proveedor, y para evitar que la autoridad emisora inicie un procedimiento de ejecución cuando ello carecería de sentido.

Si el destinatario no facilita la información, o no la facilita de forma exhaustiva o a su debido tiempo por motivos distintos de los mencionados anteriormente, deberá comunicar a la autoridad emisora los motivos, utilizando el formulario que figura en el anexo III. Los beneficiarios podrán, por tanto, plantear cualquier cuestión relacionada con la ejecución del EPOC a la autoridad emisora, lo que permite a esta corregir o reconsiderar el EPOC en una fase temprana, antes de la fase de ejecución.

Si los datos no se entregan inmediatamente, en particular cuando se haya iniciado un diálogo entre el destinatario y la autoridad emisora (lo que significa que no se respetarán los plazos del artículo 9, apartado 1), el proveedor de servicios tiene la obligación, una vez recibido el EPOC, de conservar los datos para evitar su pérdida, siempre que dichos datos puedan ser identificados. Los datos deberán conservarse con vistas a su eventual entrega en virtud de un EPOC corregido, o de una solicitud posterior mediante una orden europea de investigación o un procedimiento de asistencia jurídica mutua enviados en lugar del EPOC original.

Artículo 10: Ejecución del EPOC-PR

La ejecución de un EPOC-PR exige la conservación de los datos disponibles en el momento de la recepción de la orden. Los proveedores de servicios deberán conservar los datos durante el tiempo necesario para su entrega previa solicitud, siempre que la autoridad emisora confirme, en el plazo de 60 días después de la emisión de la orden, que ha emitido la posterior solicitud de entrega de los datos. Este proceso requiere que se hayan adoptado al menos algunas medidas formales, como el envío de una petición de asistencia judicial para la traducción.

Por otra parte, las peticiones de conservación de datos solo deberán presentarse o mantenerse durante el tiempo necesario para permitir el envío de una solicitud posterior de entrega de los datos. Para evitar que los datos se conserven innecesariamente o durante periodos excesivamente largos, la autoridad que haya emitido la orden europea de conservación deberá informar al destinatario en cuanto se tome la decisión de no emitir o de retirar una orden de entrega o una solicitud de cooperación judicial.

Esta disposición garantiza asimismo la posibilidad de diálogo entre el destinatario y la autoridad emisora, en las mismas condiciones que las definidas en el artículo 9. Si el EPOC-PR está incompleto, es manifiestamente incorrecto o no contiene información suficiente para permitir su ejecución por el proveedor de servicios, el destinatario deberá ponerse en contacto con la autoridad emisora y solicitar aclaraciones, utilizando el formulario que figura en el anexo III. También informará a la autoridad emisora en los casos en que no pueda facilitar los datos debido a fuerza mayor o imposibilidad de hecho.

Artículo 11: Confidencialidad e información al usuario

La confidencialidad de la investigación en curso, incluido el hecho de que se haya emitido una orden para obtener los datos pertinentes, debe protegerse. Este artículo se inspira en el artículo 19 de la Directiva OEI, y prevé la obligación del destinatario, y en su caso del proveedor de servicios, de proteger la confidencialidad del EPOC o del EPOC-PR, incluso absteniéndose de informar a la persona cuyos datos se solicitan cuando así lo pida la autoridad emisora, con el fin de salvaguardar la investigación de infracciones penales, de conformidad con el artículo 23 del RGPD.

También es importante, en especial para el ejercicio de las vías de recurso, informar a la persona cuyos datos se solicitan. Si esto no lo hace el proveedor de servicios a petición de la autoridad emisora, esta autoridad informará a la persona de conformidad con el artículo 13 de la Directiva sobre protección de datos en el ámbito penal, tan pronto como deje de existir el riesgo de socavar la investigación, e incluirá información sobre las vías de recurso disponibles. Debido a la menor injerencia en los derechos en cuestión, dicha información no se facilitará en caso de las órdenes europeas de conservación, sino únicamente para las órdenes europeas de entrega.

Artículo 12: Reembolso de gastos

El proveedor de servicios podrá solicitar el reembolso de sus gastos al Estado emisor, si esto está previsto en la legislación nacional de dicho Estado respecto de órdenes nacionales en situaciones comparables. Esta disposición garantiza la igualdad de trato entre los proveedores de servicios destinatarios de una orden nacional y los destinatarios de un EPOC del mismo Estado miembro, si dicho Estado ha optado por reembolsar a determinados proveedores de servicios. Por otra parte, la propuesta de Reglamento no armoniza el reembolso de gastos, puesto que los Estados miembros han tomado diferentes opciones a este respecto.

Los gastos podrán ser reclamados directamente por el proveedor de servicios o por su representante legal, y solo se reembolsarán una vez.

Capítulo 3: Sanciones y ejecución

Artículo 13: Sanciones

Los Estados miembros deberán garantizar la aplicación de multas efectivas, proporcionadas y disuasorias, cuando los proveedores de servicios no cumplan las obligaciones que les incumben en virtud de los artículos 9, 10 u 11. Esta disposición se aplicará sin perjuicio de cualquier norma nacional que prevea la imposición de sanciones penales para tales situaciones.

Artículo 14: Procedimiento de ejecución

El artículo 14 establece un procedimiento para la ejecución de las órdenes en caso de incumplimiento, con la ayuda del Estado miembro donde se encuentre el destinatario del certificado transmitido. Dependiendo del destinatario original, se tratará del Estado miembro del proveedor de servicios o del representante legal. La autoridad emisora transferirá la orden completa, incluida la justificación de la necesidad y la proporcionalidad, junto con el certificado, a la autoridad competente del Estado de ejecución, que la ejecutará de conformidad con el Derecho nacional, aplicando, en caso necesario, las sanciones a que se refiere el artículo 13. Si la orden es transmitida para su ejecución al Estado de ejecución, la

autoridad de ejecución podrá decidir no reconocer ni ejecutar la orden si, después de la recepción, considera que es aplicable alguno de los limitados motivos de oposición, y previa consulta a la autoridad emisora. Por otra parte, en caso de que se inicie el procedimiento de ejecución, el propio destinatario podrá oponerse a la orden ante la autoridad de ejecución, sobre la base de uno de estos motivos (con excepción de los privilegios e inmunidades), en particular en los casos en que sea evidente que la orden no fue emitida o validada por una autoridad competente o cuando su ejecución viole manifiestamente la Carta de los Derechos Fundamentales de la Unión Europea, o sea manifiestamente abusiva. Por ejemplo, una orden que solicite la entrega de datos de contenido que pertenezcan a una categoría indefinida de personas situadas en una zona geográfica sin un vínculo a un proceso penal concreto incumpliría manifiestamente las condiciones para la emisión de una orden europea de entrega establecidas en el presente Reglamento, lo que se apreciaría de forma evidente en el propio certificado. Otros motivos solo pueden ser invocados por la persona cuyos datos se solicitan, en el ámbito de sus propias vías de recurso en el Estado emisor (véase el artículo 17). Por otra parte, los proveedores de servicios deben tener acceso a una vía de recurso contra la resolución de la autoridad que imponga una sanción.

El procedimiento de ejecución establece varios plazos para las autoridades emisoras y de ejecución, a fin de evitar retrasos durante este procedimiento.

Capítulo 4: Vías de recurso

Artículos 15 y 16: Procedimiento de reexamen en caso de obligaciones contradictorias derivadas de la legislación de un país tercero

Los artículos 15 y 16 prevén un procedimiento de reexamen en caso de que los proveedores de servicios establecidos en países terceros se vean enfrentados a obligaciones contradictorias. Estas disposiciones también son esenciales para garantizar la protección de los derechos de las personas y el principio de cortesía internacional. Al fijar normas rigurosas, tienen por objeto alentar a los países terceros a que garanticen un nivel equivalente de protección. En la situación opuesta, cuando las autoridades de un país tercero pretendan obtener datos de un ciudadano de la UE a través de un proveedor de servicios de la UE, el Derecho de la Unión o del Estado miembro que protege los derechos fundamentales, como el acervo en materia de protección de datos, podría igualmente impedir a su divulgación. La Unión Europea espera que los países terceros respeten las prohibiciones contenidas en la presente propuesta.

El procedimiento previsto en el artículo 15 puede ser iniciado por el destinatario, si el cumplimiento de una orden europea de entrega implica una violación de la legislación de un país tercero que prohíbe la divulgación de los datos en cuestión basándose en que tal prohibición es necesaria para proteger los derechos fundamentales de los interesados o los intereses fundamentales del país tercero relacionados con la seguridad o la defensa nacionales. El destinatario estará obligado a notificar a la autoridad emisora su oposición motivada, precisando las razones por las que considera que existen obligaciones contradictorias. Esta oposición motivada no puede basarse en el mero hecho de que no existan disposiciones similares en la ley del país tercero, ni en la sola circunstancia de que los datos estén almacenados en un país tercero. La oposición motivada debe presentarse de conformidad con el procedimiento previsto en el artículo 9, apartado 5, para la notificación de la intención de no cumplir la orden, utilizando el formulario que figura en el anexo III.

Sobre la base de esta oposición motivada, la autoridad emisora reexaminará su orden. Si decide anularla, se dará por concluido el procedimiento. No obstante, si desea confirmar la orden, el caso se transferirá al órgano jurisdiccional competente de su Estado miembro, que

evaluará, sobre la base de la oposición motivada y teniendo en cuenta todos los hechos pertinentes del caso, si la legislación del país tercero se aplica en el asunto en cuestión y, en caso afirmativo, si existe conflicto. Al realizar esa evaluación, el tribunal debe tener en cuenta si la legislación del país tercero, en lugar de tener como objetivo la protección de los derechos fundamentales de las personas en cuestión o de los intereses fundamentales del país tercero relacionados con la seguridad o la defensa nacionales, aspira manifiestamente a proteger otros intereses o actividades ilícitas frente a las solicitudes de las autoridades competentes en el contexto de investigaciones penales.

Si el órgano jurisdiccional determina que existe en efecto un conflicto con las obligaciones derivadas de las leyes de protección de los derechos fundamentales de las personas o de los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, el órgano jurisdiccional deberá solicitar la opinión del país tercero a través de las autoridades centrales nacionales de dicho país. Si el país tercero consultado confirma la existencia del conflicto y se opone a la ejecución de la orden, el órgano jurisdiccional deberá retirarla.

Si el conflicto surge de otra legislación del país tercero no destinada a proteger los derechos fundamentales de las personas ni los intereses fundamentales de ese país relacionados con la seguridad y la defensa nacionales, el órgano jurisdiccional adoptará su decisión sobre la base de una ponderación de los intereses a favor y en contra de la orden.

Las condiciones establecidas en el artículo 9, y en particular las obligaciones de conservación descritas en el artículo 9, apartado 6, también son aplicables en situaciones donde surjan obligaciones contradictorias derivadas de la legislación de un país tercero. Si el órgano jurisdiccional determina que la orden debe confirmarse, la autoridad emisora y el proveedor de servicios serán informados con vistas a proceder a su ejecución. Cuando la orden se anule, podrá emitirse una orden europea de conservación independiente para garantizar la disponibilidad de datos, cuando estos puedan obtenerse a través de una petición de asistencia judicial mutua.

Habida cuenta de que la orden europea de conservación no da lugar por sí misma a la revelación de datos, y por tanto no plantea preocupaciones similares, el procedimiento de reexamen se limita a la orden europea de entrega.

Artículo 17: Vías de recurso efectivas

Esta disposición garantiza que las personas afectadas por la orden europea de entrega dispongan de vías de recurso efectivas. Estas vías de recurso se ejercen en el Estado emisor con arreglo a su legislación nacional. Para los sospechosos y acusados, los recursos se ejercen normalmente durante el proceso penal. No se establecen vías de recurso específicas para la orden europea de conservación, que por sí misma no permite la revelación de datos, excepto en los casos en que vaya seguida de una orden europea de entrega o de otro instrumento que permita la revelación de datos, lo que daría lugar a vías de recurso específicas.

Las personas cuyos datos hayan sido solicitados sin que sean sospechosas o estén acusadas en procesos penales también tendrán derecho a recurrir en el Estado emisor. Todos estos derechos se entienden sin perjuicio de las vías de recurso disponibles conforme a la Directiva sobre protección de datos en el ámbito penal y al Reglamento general de protección de datos.

A diferencia de lo que se prevé para los proveedores de servicios, el Reglamento no limita los posibles motivos de todas estas personas para impugnar la legalidad de la orden. Estos motivos incluyen la necesidad y proporcionalidad de la orden.

El ejercicio de las vías de recurso en el Estado emisor no supone una carga desproporcionada para las personas afectadas. Como ocurre con las órdenes que se ejecutan a través de otras formas de cooperación judicial, los órganos jurisdiccionales del Estado emisor están mejor situados para examinar la legalidad de las órdenes europeas de entrega emitidas por sus propias autoridades y evaluar la compatibilidad con su legislación nacional. Además, durante la fase de ejecución, los destinatarios podrán oponerse por separado a la ejecución del EPOC o del EPOC-PR en su Estado miembro de acogida basándose en una lista de motivos enumerados en el Reglamento (véase el artículo 14).

Artículo 18: Respeto de los privilegios e inmunidades en virtud de la legislación del Estado de ejecución

Esta disposición persigue, al igual que el artículo 5, apartado 7, el objetivo de garantizar que los privilegios y las inmunidades que protegen los datos solicitados en el Estado miembro del proveedor de servicios se tengan en cuenta en el Estado emisor, en particular cuando existan diferencias entre ambos Estados miembros, así como los intereses fundamentales del Estado miembro de que se trate, como la seguridad y la defensa nacionales. El artículo 18 dispone que el órgano jurisdiccional del Estado emisor debe tenerlos en cuenta como si estuvieran previstos por su legislación nacional. Debido a las diferencias entre los Estados miembros a la hora de evaluar la pertinencia y admisibilidad de las pruebas, la disposición concede cierta flexibilidad a los órganos jurisdiccionales sobre la manera de tenerlas en cuenta.

Capítulo 5: Disposiciones finales

Artículo 19: Seguimiento y presentación de informes

Este artículo obliga a los Estados miembros a comunicar información específica relacionada con la aplicación del Reglamento con el fin de asistir a la Comisión en el ejercicio de sus funciones de conformidad con el artículo 24. La Comisión elaborará un programa detallado para el seguimiento de los productos, resultados e impactos del Reglamento.

Artículo 20: Modificaciones de los certificados y formularios

Los certificados y formularios que figuran en los anexos I, II y III de la presente propuesta harán que sea más fácil ejecutar un EPOC y un EPOC-PR. Por ello, es necesario, en el futuro, poder abordar la posible necesidad de mejorar el contenido del certificado y del formulario lo más rápidamente posible. La modificación de los tres anexos mediante el procedimiento legislativo ordinario no responde a esta exigencia. Por otra parte, estos anexos constituyen elementos no esenciales de los actos legislativos, pues los elementos principales se definen en el artículo 8. Por consiguiente, en el artículo 20 se establece un procedimiento más rápido y flexible para la modificación mediante actos delegados.

Artículo 21: Ejercicio de la delegación

Este artículo establece las condiciones en las que la Comisión está facultada para adoptar actos delegados a fin de efectuar las modificaciones necesarias del certificado y de los formularios adjuntos a la propuesta. Establece un procedimiento normalizado para la adopción de tales actos delegados.

Artículo 22: Notificaciones

Los Estados miembros están obligados a notificar a la Comisión sus autoridades emisoras y de ejecución competentes, así como los órganos jurisdiccionales competentes para entender de las oposiciones motivadas de los proveedores de servicios en caso de conflicto de leyes.

Artículo 23: Relación con las órdenes europeas de investigación

Esta disposición precisa que el Reglamento no impide a las autoridades de los Estados miembros emitir órdenes europeas de investigación de conformidad con la Directiva 2014/41/UE a fin de obtener pruebas electrónicas.

Artículo 24: Evaluación

En virtud de esta disposición, la Comisión realizará una evaluación del presente Reglamento en consonancia con las directrices para la mejora de la legislación y de conformidad con el apartado 22 del Acuerdo Interinstitucional de 13 de abril de 2016[25]. La Comisión presentará un informe al Parlamento Europeo y al Consejo sobre los resultados de la evaluación, incluida una apreciación de la necesidad de ampliar su ámbito de aplicación a los servicios no cubiertos todavía, pero que puedan ser más pertinentes para las investigaciones, cinco años después de la entrada en vigor del Reglamento propuesto.

Artículo 25: Entrada en vigor

El Reglamento propuesto entrará en vigor veinte días después de su publicación en el Diario Oficial. Deberá aplicarse seis meses después de su fecha de entrada en vigor.

[25] Acuerdo Interinstitucional entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea sobre la mejora de la legislación, de 13 de abril de 2016, DO L 123 de 12.5.2016, p. 1.

2018/0108 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 82, apartado 1,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[26],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) La Unión se ha fijado el objetivo de mantener y desarrollar un espacio de libertad, seguridad y justicia. Para el establecimiento progresivo de dicho espacio, la Unión debe adoptar medidas relativas a la cooperación judicial en materia penal, basándose en el principio de reconocimiento mutuo de las sentencias y resoluciones judiciales, que es considerado comúnmente como la piedra angular de la cooperación judicial en materia penal en la Unión desde el Consejo Europeo de Tampere de 15 y 16 de octubre de 1999.

(2) Las medidas para obtener y conservar pruebas electrónicas son cada vez más importantes para poder efectuar investigaciones penales e impulsar procesos penales en toda la Unión. Unos mecanismos eficaces para obtener pruebas electrónicas son esenciales para combatir la delincuencia, siempre que se respeten unas condiciones que garanticen la plena conformidad con los derechos fundamentales y los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea y consagrados en los Tratados, en particular, los principios de necesidad y proporcionalidad, las garantías procesales, la protección de datos, la confidencialidad de la correspondencia y la intimidad.

(3) La Declaración conjunta, de 22 de marzo de 2016, de los ministros de Justicia e Interior y de los representantes de las instituciones de la Unión Europea sobre los atentados terroristas de Bruselas subrayó la necesidad, como cuestión prioritaria, de encontrar formas de obtener y asegurar pruebas electrónicas de forma más rápida y eficaz, y de establecer medidas concretas para abordar este asunto.

(4) Las conclusiones del Consejo de 9 de junio de 2016 subrayaron la importancia creciente de las pruebas electrónicas en los procesos penales, y de proteger el ciberespacio de los abusos y las actividades delictivas, lo que beneficiará a las

[26] DO C […] de […], p. […].

economías y las sociedades europeas y, por tanto, la necesidad de que las autoridades policiales y judiciales dispongan de herramientas eficaces para investigar y enjuiciar los actos delictivos relacionados con el ciberespacio.

(5) En la Comunicación conjunta sobre resiliencia, disuasión y defensa, de 13 de septiembre de 2017[27], la Comisión destacó que la investigación y el enjuiciamiento efectivos de los delitos relacionados con el ámbito cibernético constituyen un importante efecto disuasorio para los ciberataques, y que el marco procesal actual precisa estar mejor adaptado a la era de internet. Los procesos actuales a veces no logran adaptarse a la velocidad de los ciberataques, lo que crea una necesidad concreta de una cooperación transfronteriza ágil.

(6) El Parlamento Europeo se hizo eco de estas consideraciones en su Resolución sobre la lucha contra la ciberdelincuencia de 3 de octubre de 2017[28], poniendo de relieve las dificultades que el actual marco jurídico fragmentado puede crear para los proveedores de servicios que desean cumplir los requerimientos de las autoridades y pidiendo a la Comisión que propusiese un marco jurídico de la Unión para las pruebas electrónicas con las suficientes garantías para los derechos y las libertades de todos los interesados.

(7) Los servicios basados en la red pueden prestarse desde cualquier lugar y no requieren una infraestructura física, instalaciones o personal en el país en cuestión. En consecuencia, las pruebas pertinentes a menudo se almacenan fuera del Estado investigador o por un proveedor de servicios establecido fuera de dicho Estado. Con frecuencia, no existe ninguna otra vinculación entre el caso investigado en el Estado en cuestión y el Estado del lugar de almacenamiento o de establecimiento principal del proveedor del servicio.

(8) Debido a esta falta de vinculación, las solicitudes de cooperación judicial se remiten frecuentemente a Estados que acogen a un gran número de proveedores de servicios, pero que no tienen relación con el asunto en cuestión. Además, el número de solicitudes se ha multiplicado debido al mayor uso de servicios en red, que por su naturaleza no tienen fronteras. En consecuencia, la obtención de pruebas electrónicas utilizando los canales de cooperación judicial a menudo lleva mucho tiempo, más del tiempo en que podrían estar disponibles los indicios. Por otra parte, no existe un marco claro para la cooperación con los proveedores de servicios, mientras que algunos proveedores de países terceros aceptan solicitudes directas de datos sin contenido si lo permite su legislación nacional aplicable. Por ello, todos los Estados miembros dependen de la cooperación con los proveedores de servicios cuando se disponga de tal vía, utilizando diferentes instrumentos, condiciones y procedimientos nacionales. Además, para los datos de contenido, algunos Estados miembros han adoptado medidas unilaterales, mientras que otros siguen confiando en la cooperación judicial.

(9) El fragmentado marco jurídico supone una dificultad para los proveedores de servicios que desean cumplir los requerimientos de las autoridades. Por tanto, es preciso establecer un marco jurídico europeo relativo a las pruebas electrónicas que obligue a los proveedores de servicios cubiertos por el instrumento a responder directamente a las autoridades sin la intervención de un órgano judicial en el Estado miembro del proveedor del servicio.

---

27 JOIN(2017) 450 final.

28 2017/2068(INI).

(10) Las órdenes en virtud del presente Reglamento deben remitirse a los representantes legales de los proveedores de servicios designados para tal fin. Si un proveedor de servicios establecido en la Unión no ha designado un representante legal, las órdenes podrán remitirse a cualquier establecimiento de dicho proveedor en la Unión. Esta opción alternativa sirve para garantizar la eficacia del sistema en caso de que el proveedor de servicios no haya designado (todavía) un representante específico.

(11) El mecanismo de la orden europea de entrega y la orden europea de conservación de pruebas electrónicas a efectos de enjuiciamiento penal solo puede funcionar con un alto nivel de confianza mutua entre los Estados miembros, que es un presupuesto esencial para el buen funcionamiento de este instrumento.

(12) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. Entre estos se incluyen el derecho a la libertad y a la seguridad, el respeto de la vida privada y familiar, la protección de los datos de carácter personal, la libertad de empresa, el derecho a la propiedad, el derecho a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia y el derecho a la defensa, los principios de legalidad y de proporcionalidad, así como el derecho a no ser juzgado o condenado penalmente dos veces por el mismo delito. En caso de que el Estado miembro emisor tenga indicios de que un proceso penal paralelo puede estar en curso en otro Estado miembro, consultará a las autoridades de dicho Estado miembro de conformidad con la Decisión marco 2009/948/JAI del Consejo[29].

(13) A fin de garantizar el pleno respeto de los derechos fundamentales, el presente Reglamento se refiere de manera explícita a las normas necesarias relativas a la obtención de datos personales, el tratamiento de estos datos, el control judicial de la utilización de la medida de investigación facilitada por este instrumento, así como las vías de recurso disponibles.

(14) El presente Reglamento deberá aplicarse sin perjuicio de los derechos procesales en los procesos penales previstos en las Directivas 2010/64/UE[30], 2012/13/UE[31], 2013/48/UE[32], 2016/343[33], 2016/800[34] y 2016/1919[35] del Parlamento Europeo y del Consejo.

---

29 Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, DO L 328 de 15.12.2009, p. 42.

30 Directiva 2010/64/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, relativa al derecho a interpretación y a traducción en los procesos penales, DO L 280 de 26.10.2010, p. 1.

31 Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales, DO L 142 de 1.6.2012, p. 1.

32 Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad, DO L 294 de 6.11.2013, p. 1.

33 Directiva (UE) 2016/343 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio, DO L 65 de 11.3.2016, p. 1.

34 Directiva (UE) 2016/800 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales, DO L 132 de 21.5.2016, p. 1.

(15) El presente instrumento establece las normas en virtud de las cuales una autoridad judicial competente de la Unión Europea podrá ordenar a un proveedor de servicios que ofrezca servicios en la Unión, por medio de una orden europea de entrega o de conservación, que entregue o conserve pruebas electrónicas. El presente Reglamento será aplicable en todos los casos en que el proveedor de servicios esté establecido o representado en otro Estado miembro. En contextos nacionales en los que no puedan utilizarse los instrumentos establecidos en virtud del presente Reglamento, el Reglamento no deberá limitar los poderes de las autoridades nacionales competentes ya fijados por la legislación nacional para obligar a los proveedores de servicios establecidos o representados en su territorio.

(16) Los proveedores de servicios más importantes a efectos de recabar pruebas para procesos penales son los proveedores de servicios de comunicaciones electrónicas y los proveedores de servicios de la sociedad de la información que facilitan específicamente la interacción entre usuarios. Así pues, ambos grupos deben estar cubiertos por el presente Reglamento. Los servicios de comunicaciones electrónicas se definen en la propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas. Aquí se incluyen las comunicaciones interpersonales tales como los servicios de voz sobre IP, los servicios de mensajería instantánea y los servicios de correo electrónico. Las categorías de servicios de la sociedad de la información aquí incluidos son aquellos que cuentan con el almacenamiento de datos como componente esencial del servicio prestado al usuario, y se refieren en particular a las redes sociales en la medida en que no puedan calificarse como servicios de comunicaciones electrónicas, los mercados en línea que facilitan transacciones entre sus usuarios (como consumidores o empresas) y otros servicios de alojamiento de datos, incluso en los casos en que el servicio se presta a través de la computación en la nube. Los servicios de la sociedad de la información que no cuentan con el almacenamiento de datos como componente esencial del servicio prestado al usuario, y para los que solo es de carácter secundario, como los servicios jurídicos, de arquitectura, de ingeniería y de contabilidad prestados en línea a distancia, deben quedar excluidos del ámbito de aplicación del presente Reglamento, aun cuando puedan corresponder a la definición de servicios de la sociedad de la información según lo establecido en la Directiva (UE) 2015/1535.

(17) En muchos casos, los datos ya no se almacenan o tratan en un dispositivo del usuario, sino que están disponibles en una infraestructura en la nube que permite acceder a ellos desde cualquier lugar. Para gestionar estos servicios, no es necesario que los proveedores de servicios estén establecidos o tengan servidores en un territorio específico. Por tanto, la aplicación del presente Reglamento no debe depender de la localización efectiva del establecimiento del proveedor o de la instalación de tratamiento o almacenamiento de datos.

(18) Los proveedores de servicios de infraestructura de internet relacionados con la asignación de nombres y números, como los registros y registradores de nombres de dominio y los proveedores de servicios de privacidad y representación, o los registros regionales de direcciones de protocolo de internet (direcciones IP), revisten especial importancia en lo que respecta a la identificación de quienes están detrás de las

---

35 Directiva (UE) 2016/1919 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, relativa a la asistencia jurídica gratuita a los sospechosos y acusados en los procesos penales y a las personas buscadas en virtud de un procedimiento de orden europea de detención, DO L 297 de 4.11.2016, p. 1.

páginas web maliciosas o comprometidas. Estos proveedores disponen de datos que revisten especial relevancia para las investigaciones penales, ya que pueden permitir la identificación de una persona física o jurídica responsable de un sitio web utilizado en actividades delictivas, o la identificación de la víctima de la actividad delictiva en el caso de un sitio web comprometido que haya sido secuestrado por delincuentes.

(19) El presente Reglamento regula únicamente la obtención de datos almacenados, es decir, de datos que obren en poder de un proveedor de servicios en el momento en que reciba un certificado de orden europea de entrega o de conservación. No establece una obligación general de conservación de datos, ni tampoco autoriza la interceptación de datos o la obtención de datos almacenados en un momento futuro a partir de la recepción de un certificado de orden europea de entrega o de conservación. Los datos deberán entregarse, independientemente de si están cifrados o no.

(20) Las categorías de datos cubiertos por el presente Reglamento incluyen los datos de los abonados, los datos relativos al acceso y los datos de transacciones (categorías denominadas «datos sin contenido»), así como los datos de contenido. Esta distinción, aparte de los datos relativos al acceso, existe en la legislación de muchos Estados miembros y también en el actual marco jurídico de los Estados Unidos, que permite a los proveedores de servicios compartir voluntariamente datos sin contenido con autoridades policiales y judiciales extranjeras.

(21) Procede considerar los datos relativos al acceso como una categoría específica de datos utilizada en el presente Reglamento. Los datos relativos al acceso se buscan con el mismo objetivo que los datos de los abonados, es decir, para identificar al usuario subyacente, y el nivel de interferencia con los derechos fundamentales es similar al de los datos de los abonados. Los datos relativos al acceso se registran normalmente como parte de un registro de acontecimientos (en otras palabras, un registro de servidor) para indicar el comienzo y el fin de la sesión de acceso de un usuario a un servicio. A menudo es una dirección IP (estática o dinámica) u otro identificador el que señala la interfaz de red utilizada durante la sesión de acceso. Si el usuario es desconocido, a menudo debe obtenerse este identificador antes de que puedan pedirse al proveedor de servicios los datos de abonado correspondientes a dicho identificador.

(22) Los datos de transacciones, por el contrario, suelen buscarse para obtener información sobre los contactos y el paradero del usuario, y pueden servir para establecer el perfil de un individuo. Por otro lado, los datos relativos al acceso no sirven por sí solos para un objetivo similar; por ejemplo, no revelan ninguna información sobre los interlocutores relacionados con el usuario. Por consiguiente, la presente propuesta introduce una nueva categoría de datos, que debe tratarse como los datos de los abonados si el objetivo de la obtención de estos datos es similar.

(23) Todas las categorías de datos contienen datos personales, y están por tanto cubiertas por las garantías establecidas en el acervo de la Unión sobre protección de datos, pero la intensidad del impacto en los derechos fundamentales varía, en particular entre los datos de los abonados y los datos relativos al acceso por una parte, y los datos de transacciones y los datos de contenido, por otra. Mientras que los datos de los abonados y los datos relativos al acceso son útiles para obtener unos primeros indicios en una investigación sobre la identidad de un sospechoso, los datos de transacciones y los datos de contenido son más relevantes como material probatorio. Es por tanto esencial que todas estas categorías de datos estén cubiertas por el instrumento. Debido al distinto grado de injerencia en los derechos fundamentales, se imponen condiciones

diferentes para obtener datos de los abonados y datos relativos al acceso por una parte, y datos de transacciones y datos de contenido, por otra.

(24) La orden europea de entrega y la orden europea de conservación son medidas de investigación que deben emitirse únicamente en el marco de procesos penales específicos contra los autores concretos, conocidos o aún desconocidos, de una infracción penal que ya haya tenido lugar, tras una evaluación individual de la proporcionalidad y la necesidad en cada caso concreto.

(25) El presente Reglamento se entiende sin perjuicio de los poderes de investigación de las autoridades en procedimientos administrativos o civiles, en particular cuando dichos procedimientos puedan dar lugar a sanciones.

(26) El presente Reglamento deberá aplicarse a los proveedores de servicios en la Unión, y las órdenes previstas por el presente Reglamento solo podrán emitirse respecto de los datos relativos a servicios ofrecidos en la Unión. Los servicios ofrecidos exclusivamente fuera de la Unión no entran en el ámbito de aplicación del presente Reglamento, incluso en el caso de que el proveedor de servicios esté establecido en la Unión.

(27) La determinación de si un proveedor ofrece servicios en la Unión requiere una evaluación de si el proveedor permite a las personas físicas o jurídicas que se encuentren en uno o más Estados miembros utilizar sus servicios. No obstante, la mera accesibilidad de una interfaz en línea (como por ejemplo la accesibilidad de la página web del proveedor de servicios o de un intermediario, o de una dirección de correo electrónico y otros datos de contacto) en uno o más Estados miembros considerada aisladamente no debe ser una condición suficiente para la aplicación del presente Reglamento.

(28) Una estrecha vinculación con la Unión deberá también ser pertinente para determinar el ámbito de aplicación del presente Reglamento. Debe considerarse que existe tal estrecha vinculación cuando el proveedor tenga un establecimiento en la Unión. A falta de tal establecimiento, el criterio de la estrecha vinculación debe evaluarse sobre la base de la existencia de un número significativo de usuarios en uno o más Estados miembros, o la orientación de las actividades hacia uno o más Estados miembros. La orientación de las actividades hacia uno o más Estados miembros puede determinarse en función de todas las circunstancias pertinentes, incluidos factores como el uso de una lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar bienes o servicios. La orientación de las actividades hacia un Estado miembro también puede derivarse de la disponibilidad de una aplicación para móvil en la tienda de aplicaciones nacional, de la publicidad local o la publicidad en la lengua utilizada en dicho Estado miembro, o de la gestión de las relaciones con los clientes, como la prestación de servicios a los clientes en la lengua comúnmente utilizada en tal Estado miembro. También se supone una estrecha vinculación cuando un proveedor de servicios dirige su actividad hacia uno o varios Estados miembros con arreglo a lo establecido en el artículo 17, apartado 1, letra c), del Reglamento n.º 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[36]. Por otra parte, la prestación del servicio con vistas a la mera observancia de la prohibición de discriminación

[36] Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, DO L 351 de 20.12.2012, p. 1.

establecida en el Reglamento (UE) 2018/302[37] no puede, por este único motivo, considerarse que dirige u orienta las actividades hacia un territorio determinado de la Unión.

(29) Una orden europea de entrega solo debe emitirse si es necesario y proporcionado. La evaluación deberá tener en cuenta si la orden se limita a lo estrictamente necesario para alcanzar el objetivo legítimo de la obtención de datos relevantes y necesarios para servir de prueba solo en un caso concreto.

(30) En el proceso de emisión o de validación de una orden europea de entrega o de conservación siempre deberá intervenir una autoridad judicial. Habida cuenta del carácter especialmente sensible de los datos de transacciones y los datos de contenido, la emisión o validación de las órdenes europeas de entrega para estas categorías de datos requiere la supervisión de un juez. Puesto que los datos de abonado y los datos relativos al acceso son menos sensibles, las órdenes europeas de entrega a efectos de su revelación pueden además ser emitidas o validadas por fiscales competentes.

(31) Por la misma razón, es preciso hacer una distinción en relación al ámbito de aplicación material del presente Reglamento. Las órdenes para entregar datos de los abonados y datos relativos al acceso pueden emitirse para cualquier infracción penal, mientras que el acceso a los datos de transacciones y los datos de contenido debe estar sujeto a requisitos más estrictos para reflejar el carácter más sensible de estos datos. Un umbral permite un enfoque más proporcionado, junto con una serie de condiciones previas y *a posteriori* y las salvaguardias previstas en el presente Reglamento con el fin de garantizar el respeto de la proporcionalidad y los derechos de las personas afectadas. Al mismo tiempo, el umbral no debe limitar la eficacia del instrumento y su uso por los profesionales. Permitir la emisión de órdenes para la investigación de delitos que lleven aparejada una pena máxima de privación de libertad de al menos tres años, limita el alcance del instrumento a los delitos más graves, sin afectar excesivamente a las posibilidades de uso por los profesionales. Este umbral excluye del ámbito de aplicación un gran número de delitos que los Estados miembros consideran menos graves, tal como se desprende de su pena máxima inferior. También tiene la ventaja de ser fácilmente aplicable en la práctica.

(32) Existen determinadas infracciones para las que las pruebas estarán normalmente disponibles solo en formato electrónico, que por su naturaleza es especialmente fugaz. Este es el caso de los delitos relacionados con el ámbito cibernético, incluso los que no pueden considerarse graves en sí mismos, pero que pueden causar daños extensos o considerables, en particular los casos con limitado impacto individual, pero de elevado volumen y perjuicio general. En la mayoría de los casos en que la infracción se haya cometido por medio de un sistema de información, la aplicación del mismo umbral que para otros tipos de infracciones daría lugar a la impunidad. Esto justifica la aplicación del Reglamento también a las infracciones a las que corresponda una pena inferior a tres años de privación de libertad. Asimismo, los delitos relacionados con el terrorismo, según lo descrito en la Directiva (UE) 2017/541, no exigen el umbral de pena máxima de privación de libertad de al menos tres años.

---

37 Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.° 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE, DO LI 60 de 2.3.2018, p. 1.

(33) Además, es necesario prever que la orden europea de entrega solo podrá emitirse si, para la misma infracción penal en una situación nacional comparable en el Estado emisor, estaría disponible una orden similar.

(34) En los casos en que los datos solicitados se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa u otra entidad distinta de las personas físicas, lo que suele ocurrir en el caso de los servicios de alojamiento, la orden europea de entrega solo podrá utilizarse cuando otras medidas de investigación dirigidas a la empresa o la entidad no sean adecuadas, en particular porque podrían poner en peligro la investigación. Esto es pertinente, en particular, por lo que se refiere a las entidades de mayor tamaño, como sociedades anónimas o entidades públicas, que recurren a servicios de proveedores para sus infraestructuras o servicios informáticos, o ambas cosas. El primer destinatario de una orden europea de entrega, en tales situaciones, debe ser la empresa u otra entidad. Esta empresa u otra entidad puede no ser un proveedor de servicios cubierto por el ámbito de aplicación del presente Reglamento. No obstante, en los casos en que no sea oportuno dirigirse a dicha entidad, por ejemplo porque se sospeche de su implicación en el asunto en cuestión o si hay indicios de colusión con el objetivo de la investigación, las autoridades competentes deberán poder dirigirse al proveedor de servicios que proporcione la infraestructura en cuestión para que facilite los datos solicitados. Esta disposición no afecta al derecho a ordenar al proveedor de servicios que conserve los datos.

(35) Los privilegios e inmunidades referidos a determinadas categorías de personas (por ejemplo, los diplomáticos) o a relaciones específicamente protegidas (prerrogativa de secreto profesional en la relación abogado-cliente) están contemplados en otros instrumentos de reconocimiento mutuo, como la orden europea de investigación. Su alcance y su impacto difieren según la legislación nacional aplicable, que deberá tenerse en cuenta en el momento de emitir la orden, dado que la autoridad emisora solo podrá emitirla si en una situación comparable a nivel nacional estuviera disponible una orden similar. Además de este principio básico, los privilegios e inmunidades que protegen los datos relativos al acceso, los datos de transacciones o los datos de contenido en el Estado miembro del proveedor del servicio, deben tenerse en cuenta en la medida de lo posible en el Estado emisor de la misma manera que si estuvieran previstos en la legislación nacional del Estado emisor. Esto es relevante, en particular, en caso de que la legislación del Estado miembro en el que el prestador de servicios o su representante legal sean requeridos ofrezca una mayor protección que la legislación del Estado emisor. La disposición también contempla los casos en que la revelación de los datos pueda afectar a intereses fundamentales de dicho Estado miembro, como la seguridad y defensa nacionales. Como salvaguardia adicional, la autoridad de ejecución deberá tener en cuenta estos aspectos, no solo en el momento de emitirse la orden, sino también posteriormente, al evaluar la pertinencia y la admisibilidad de los datos en cuestión en la fase pertinente del proceso penal, y en caso de que se haya iniciado un procedimiento de ejecución.

(36) La orden europea de conservación podrá emitirse para cualquier infracción. Su objetivo es evitar la eliminación, supresión o modificación de los datos pertinentes en situaciones en las que puede llevar más tiempo conseguir la entrega de estos datos, por ejemplo porque se utilicen los canales de cooperación judicial.

(37) Las órdenes europeas de entrega y conservación deberán remitirse al representante legal designado por el proveedor de servicios. En ausencia de un representante legal designado, las órdenes podrán remitirse a un establecimiento del proveedor de

servicios en la Unión. Este puede ser el caso cuando el proveedor de servicios no tenga la obligación de designar un representante legal. En caso de incumplimiento por el representante legal en situaciones urgentes, la orden europea de entrega o de conservación también podrá remitirse al proveedor de servicios a la vez que se adoptan medidas de ejecución de la orden original, o en vez de adoptar dichas medidas, de conformidad con el artículo 14. En caso de incumplimiento por el representante legal en casos no urgentes, pero cuando existan riesgos claros de pérdida de datos, la orden europea de entrega o de conservación también podrá remitirse a cualquier establecimiento del proveedor en la Unión. Debido a estas distintas situaciones posibles, en las disposiciones se utiliza el término general «destinatario». Cuando una obligación, por ejemplo en materia de confidencialidad, se aplique no solo al destinatario, sino también al proveedor de servicios en caso de que no sea el destinatario, esto se especificará en la disposición correspondiente.

(38) Las órdenes europeas de entrega y las órdenes europeas de conservación deberán transmitirse al proveedor del servicio a través de un certificado de orden europea de entrega (EPOC) o un certificado de orden europea de conservación (EPOC-PR), que deberán traducirse. Los certificados deberán contener la misma información obligatoria que las órdenes, salvo en lo que respecta a la justificación de la necesidad y proporcionalidad de la medida o información complementaria sobre el caso a fin de evitar poner en peligro la investigación, pero dado que forman parte de la propia orden, permiten al sospechoso impugnarla posteriormente durante el proceso penal. En caso necesario, los certificados deberán traducirse a la lengua oficial del Estado miembro del destinatario, o a una de ellas, o a otra lengua oficial que el proveedor del servicio haya declarado aceptar.

(39) La autoridad emisora competente deberá transmitir el EPOC o el EPOC-PR directamente al destinatario por cualquier medio que pueda dejar constancia escrita, en condiciones que permitan al proveedor del servicio verificar su autenticidad, como el correo certificado, correo electrónico seguro, plataformas u otras vías seguras, incluidas las puestas a disposición por el proveedor de servicios, de conformidad con las normas sobre protección de los datos personales.

(40) La información solicitada deberá transmitirse a las autoridades en un plazo máximo de 10 días a partir de la recepción del EPOC. El proveedor deberá respetar plazos más breves en casos urgentes y si la autoridad emisora indica otros motivos para desviarse del plazo de 10 días. Además del peligro inminente de supresión de los datos solicitados, tales motivos podrían incluir circunstancias relacionadas con una investigación en curso, por ejemplo cuando los datos solicitados estén asociados a otras medidas de investigación urgentes que no puedan realizarse sin los datos en cuestión o que dependan de ellos de otro modo.

(41) Para que los proveedores de servicios puedan hacer frente a problemas formales, es necesario establecer un procedimiento para la comunicación entre el proveedor de servicios y la autoridad judicial emisora en los casos en que el EPOC esté incompleto, contenga errores manifiestos, o no contenga información suficiente para ejecutar la orden. Además, en caso de que el proveedor de servicios no pueda facilitar la información de manera exhaustiva u oportuna por cualquier otro motivo (por ejemplo, porque considere que existe un conflicto con una obligación derivada de la legislación de un país tercero, o porque considere que la orden europea de entrega no se ha emitido de conformidad con las condiciones establecidas por el presente Reglamento), deberá ponerse en contacto con la autoridad emisora y ofrecer las justificaciones oportunas. El procedimiento de comunicación deberá por tanto permitir en términos

generales la corrección o la revisión del EPOC por la autoridad emisora en un estadio inicial. Para garantizar la disponibilidad de los datos, el proveedor de servicios deberá conservarlos siempre que pueda identificar los datos requeridos.

(42) Tras la recepción de un certificado de orden europea de conservación (EPOC-PR), el proveedor de servicios deberá conservar los datos solicitados durante un máximo de 60 días, a menos que la autoridad emisora le informe de que ha puesto en marcha el procedimiento para emitir una solicitud posterior de entrega, en cuyo caso la conservación deberá mantenerse. Se considera que este período de 60 días permite la puesta en marcha de una solicitud oficial. Para ello se requiere que se hayan adoptado al menos algunas medidas formales, por ejemplo el envío de una petición de asistencia judicial mutua para traducción. Tras la recepción de dicha información, los datos deberán conservarse el tiempo que sea necesario hasta que se entreguen en el marco de una solicitud posterior de entrega.

(43) Los proveedores de servicios y sus representantes legales deberán garantizar la confidencialidad y, cuando así lo solicite la autoridad emisora, abstenerse de informar a la persona cuyos datos se solicitan a fin de salvaguardar la investigación de infracciones penales, de conformidad con el artículo 23 del Reglamento (UE) 2016/679[38]. No obstante, la información sobre el usuario es un elemento esencial para permitir el control jurisdiccional y el recurso judicial y debe ser facilitada por la autoridad si al proveedor de servicios se le ha pedido que no informe al usuario, cuando no haya riesgo de poner en peligro las investigaciones en curso, con arreglo a lo dispuesto en la norma nacional de aplicación del artículo 13 de la Directiva (UE) 2016/680[39].

(44) En caso de incumplimiento por parte del destinatario, la autoridad emisora podrá trasladar la orden completa, incluida la justificación con respecto a la necesidad y la proporcionalidad, junto con el certificado, a la autoridad competente del Estado miembro en el que resida o esté establecido el destinatario del certificado. Este Estado miembro deberá ejecutarla de conformidad con su legislación nacional. Los Estados miembros deberán prever la imposición de sanciones pecuniarias efectivas, proporcionadas y disuasorias en caso de incumplimiento de las obligaciones que establece el presente Reglamento.

(45) El procedimiento de ejecución es un procedimiento por el que el destinatario puede oponerse a la ejecución en virtud de determinados motivos restringidos. La autoridad de ejecución podrá negarse a reconocer y ejecutar la orden por los mismos motivos, o si se aplican privilegios e inmunidades con arreglo a su legislación nacional, o si la revelación puede afectar a sus intereses fundamentales, como la seguridad y defensa nacionales. La autoridad de ejecución deberá consultar a la autoridad emisora antes de negarse a reconocer o ejecutar la orden, sobre la base de esos motivos. En caso de incumplimiento, las autoridades podrán imponer sanciones. Estas sanciones deberán

---

38 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1.

39 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 de 4.5.2016, p. 89.

ser proporcionadas, también a la vista de circunstancias específicas tales como el incumplimiento repetido o sistemático.

(46) Sin perjuicio de sus obligaciones en materia de protección de datos, los proveedores de servicios no deberán considerarse responsables en los Estados miembros por el perjuicio causado a sus usuarios o a terceras partes derivado exclusivamente del cumplimiento de buena fe de un EPOC o un EPOC-PR.

(47) Además de las personas cuyos datos se solicitan, los proveedores de servicios y los países terceros pueden verse afectados por la medida de investigación. Para garantizar la cortesía con respecto a los intereses soberanos de países terceros, proteger a la persona de que se trate y hacer frente a obligaciones contradictorias de los proveedores de servicios, este instrumento prevé un mecanismo específico de revisión judicial cuando el cumplimiento de una orden europea de entrega impida a los proveedores de servicios cumplir una obligación jurídica derivada de la legislación de un país tercero.

(48) A tal fin, cuando el destinatario considere que la orden europea de entrega en el caso concreto implicaría la violación de una obligación legal derivada de la legislación de un país tercero, deberá informar a la autoridad emisora por medio de una objeción motivada, utilizando para ello los formularios previstos. La autoridad emisora deberá revisar la orden europea de entrega a la luz de la objeción motivada, teniendo en cuenta los mismos criterios que tendría que seguir el órgano jurisdiccional competente. Cuando la autoridad decida mantener la orden, el procedimiento deberá remitirse al órgano jurisdiccional competente, según lo notificado por el Estado miembro de que se trate, que procederá a una revisión de la orden.

(49) Al determinar la existencia de una obligación contradictoria en las circunstancias concretas del caso en cuestión, el órgano jurisdiccional competente deberá recurrir, cuando sea necesario, a asesoramiento externo adecuado, por ejemplo si la revisión plantea cuestiones relativas a la interpretación de la legislación del país tercero de que se trate. Esto podría incluir la consulta a las autoridades centrales de dicho país.

(50) El asesoramiento especializado sobre la interpretación podría facilitarse también por medio de opiniones de expertos, cuando estén disponibles. La información y la jurisprudencia sobre la interpretación de la legislación de países terceros y sobre los procedimientos de conflictos en los Estados miembros deberán publicarse en una plataforma central como el proyecto SIRIUS o la Red Judicial Europea. Esto permitirá a los órganos jurisdiccionales beneficiarse de la experiencia y los conocimientos acumulados por otros órganos jurisdiccionales sobre cuestiones idénticas o similares. Ello no impedirá una nueva consulta del país tercero cuando proceda.

(51) En los casos en que existan obligaciones contradictorias, el órgano jurisdiccional deberá determinar si las disposiciones contradictorias del país tercero prohíben la revelación de los datos en cuestión porque sea necesario para proteger los derechos fundamentales de las personas en cuestión o los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales. Al realizar esta apreciación, el órgano jurisdiccional deberá tener en cuenta si la legislación del país tercero, en lugar de dirigirse a proteger los derechos fundamentales o los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, busca manifiestamente proteger otros intereses o pretende amparar actividades ilegales frente a requerimientos policiales en el contexto de investigaciones penales. Si el órgano jurisdiccional concluye que las disposiciones contradictorias del país tercero prohíben la revelación de los datos porque es necesario para proteger los derechos fundamentales de las personas en cuestión o los intereses fundamentales del país

tercero relacionados con la seguridad y la defensa nacionales, deberá consultar al país tercero a través de sus autoridades centrales, ya establecidas a efectos de asistencia judicial mutua en la mayor parte del mundo. Deberá establecer un plazo para que el país tercero formule objeciones contra la ejecución de la orden europea de entrega; en caso de que las autoridades del país tercero no contesten en el plazo (prorrogado) a pesar de habérseles enviado un recordatorio informando de las consecuencias de no responder, el órgano jurisdiccional confirmará la orden. Si las autoridades del país tercero se oponen a la revelación, el órgano jurisdiccional deberá anular la orden.

(52) En todos los demás casos de obligaciones contradictorias, no vinculadas a los derechos fundamentales de la persona o a intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, el órgano jurisdiccional deberá decidir sobre la conveniencia de confirmar la orden europea de entrega, ponderando una serie de elementos concebidos para determinar la fuerza de la vinculación con cualquiera de las dos jurisdicciones afectadas, sus intereses respectivos para obtener o impedir la revelación de los datos, y las posibles consecuencias para el proveedor de servicios de tener que cumplir la orden. En el caso de las infracciones relacionadas con el ámbito cibernético, el lugar donde se cometió el delito abarca tanto el lugar o lugares donde tuvo lugar la acción como el lugar o lugares donde se materializaron los efectos de la infracción.

(53) Las condiciones establecidas en el artículo 9 serán aplicables también cuando existan obligaciones contradictorias derivadas de la legislación de un país tercero. Durante este procedimiento, los datos deberán conservarse. Si la orden se anula, podrá emitirse una nueva orden de conservación para permitir que la autoridad emisora solicite la entrega de los datos a través de otros canales, como la asistencia jurídica mutua.

(54) Es esencial que todas las personas cuyos datos se solicitan en investigaciones o procesos penales tengan acceso a una tutela judicial efectiva, de conformidad con el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea. Para los sospechosos y acusados, el derecho a una tutela judicial efectiva deberá ejercerse durante el proceso penal. Esto puede afectar a la admisibilidad, o en su caso al peso en el proceso, de las pruebas obtenidas por estos medios. Asimismo, se benefician de todas las garantías procesales aplicables a ellos, como el derecho a la información. También las personas que no sean sospechosos o acusados deberán tener derecho a la tutela judicial efectiva. Por tanto, como mínimo, deberá preverse la posibilidad de impugnar la legalidad de una orden europea de entrega, en particular su necesidad y proporcionalidad. El presente Reglamento no deberá limitar los posibles motivos para impugnar la legalidad de la orden. Estos recursos deberán ejercerse en el Estado emisor con arreglo a su legislación nacional. Las normas sobre medidas cautelares deberán regirse por la legislación nacional.

(55) Además, durante el procedimiento de ejecución y el posterior recurso judicial, el destinatario podrá oponerse a la ejecución de una orden europea de entrega o de conservación por un número limitado de motivos, entre los que figuran que no haya sido emitida o validada por una autoridad competente, que sea evidente que viola claramente la Carta de los Derechos Fundamentales de la Unión Europea, o que sea manifiestamente abusiva. Por ejemplo, una orden que solicite la entrega de datos de contenido referentes a una categoría de personas indefinida en una zona geográfica concreta, o que no tenga un vínculo con un proceso penal concreto, sería manifiesto que ignora los requisitos para emitir una orden europea de entrega.

(56) La protección de las personas físicas en el tratamiento de datos personales es un derecho fundamental. De conformidad con el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del TFUE, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Al aplicar el presente Reglamento, los Estados miembros deberán velar por que los datos personales estén protegidos y solo puedan ser tratados de conformidad con el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680.

(57) Los datos personales obtenidos en virtud del presente Reglamento deberán tratarse solo cuando sea necesario y ser proporcionados para fines de prevención, investigación, detección y enjuiciamiento de delitos, la aplicación de sanciones penales y el ejercicio de los derechos de la defensa. En particular, los Estados miembros deberán garantizar que se apliquen las políticas y medidas pertinentes en materia de protección de datos a la transmisión de datos personales de las autoridades competentes a los proveedores de servicios para los fines del presente Reglamento, así como las medidas destinadas a garantizar la seguridad de los datos. Los proveedores de servicios deberán garantizar lo mismo para la transmisión de datos personales a las autoridades pertinentes. Solo personas autorizadas deberán tener acceso a información que contenga datos de carácter personal que puedan conseguirse a través de procesos de autenticación. Deberá considerarse la utilización de mecanismos que garanticen la autenticación, como los sistemas nacionales de identificación electrónica notificados o los servicios de confianza con arreglo a lo dispuesto por el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

(58) La Comisión deberá realizar una evaluación del presente Reglamento basada en los cinco criterios de eficiencia, eficacia, pertinencia, coherencia y valor añadido de la Unión, que deberá servir de base para las evaluaciones de impacto de posibles nuevas medidas. La información deberá recabarse periódicamente y con el fin de contribuir a la evaluación del presente Reglamento.

(59) El uso de formularios pretraducidos y normalizados facilita la cooperación y el intercambio de información entre las autoridades judiciales y los proveedores de servicios, permitiéndoles asegurar y transmitir pruebas electrónicas de forma más rápida y eficaz, cumpliendo al mismo tiempo los requisitos de seguridad necesarios de forma sencilla. Reducen los costes de traducción y contribuyen a un alto nivel de calidad. Asimismo, los formularios de respuesta permiten un intercambio de información normalizado, en particular cuando los proveedores de servicios no estén en condiciones de cumplir porque la cuenta no existe o porque no se disponga de datos. Los formularios también facilitan la recogida de estadísticas.

(60) Con el fin de abordar de manera efectiva la posible necesidad de mejora en cuanto al contenido de los EPOC y los EPOC-PR y del formulario utilizado para facilitar información sobre la imposibilidad de ejecutar el EPOC o el EPOC-PR, la facultad de adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea debe delegarse en la Comisión para modificar los anexos I, II y III del presente Reglamento. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo

interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[40]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupan de la preparación de actos delegados.

(61) Las medidas basadas en el presente Reglamento no deberán sustituir a las órdenes europeas de investigación de conformidad con la Directiva 2014/41/UE del Parlamento Europeo y del Consejo[41] para obtener pruebas electrónicas. Las autoridades de los Estados miembros deberán elegir el instrumento más adaptado a su situación; podrán preferir utilizar la orden europea de investigación para solicitar un bloque de distintos tipos de medidas de investigación, incluyendo la entrega de pruebas electrónicas desde otro Estado miembro, pero sin limitarse a ello.

(62) Debido a la evolución tecnológica, en pocos años pueden prevalecer nuevas formas de instrumentos de comunicación, o pueden surgir lagunas en la aplicación del presente Reglamento. A este respecto, es importante prever una revisión de su aplicación.

(63) Dado que el objetivo del presente Reglamento, a saber, mejorar la seguridad y obtener pruebas electrónicas en un contexto transfronterizo, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a su naturaleza transfronteriza, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dichos objetivos.

(64) De conformidad con el artículo 3 del Protocolo sobre la posición del Reino Unido y de Irlanda relativo al espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, [el Reino Unido e Irlanda han notificado su deseo de participar en la adopción y en la aplicación del presente Reglamento]/[sin perjuicio de lo dispuesto en el artículo 4 de dicho Protocolo, el Reino Unido e Irlanda no participan en la adopción del presente Reglamento y no quedan vinculados por este ni sujetos a su aplicación].

(65) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción del presente Reglamento y no queda vinculada por este ni sujeta a su aplicación.

(66) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.° 45/2001 del Parlamento Europeo y del Consejo[42], emitió un dictamen el [...][43].

---

40 DO L 123 de 12.5.2006, p. 1.

41 Directiva 2014/41/UE, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, DO L 130 de 1.5.2014, p. 1.

42 Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO L 8 de 12.1.2001, p. 1.

43 DO C […] de […], p. […].

HAN ADOPTADO EL PRESENTE REGLAMENTO:

Capítulo 1: Objeto, definiciones y ámbito de aplicación

Artículo 1
Objeto

1. El presente Reglamento establece las normas en virtud de las cuales una autoridad de un Estado miembro podrá ordenar a un proveedor que ofrezca servicios en la Unión, que entregue o conserve pruebas electrónicas, con independencia de la ubicación de los datos. El presente Reglamento se entiende sin perjuicio de las competencias de las autoridades nacionales para obligar a los proveedores de servicios establecidos o representados en su territorio a acatar medidas nacionales similares.

2. El presente Reglamento no podrá tener por efecto modificar la obligación de respetar los derechos fundamentales y los principios jurídicos consagrados en el artículo 6 del TUE, incluido el derecho de defensa de las personas incursas en un proceso penal; cualesquiera obligaciones que correspondan a las autoridades policiales o judiciales a este respecto permanecerán inmutables.

Artículo 2
Definiciones

A efectos del presente Reglamento, se aplicarán las definiciones siguientes:

(1) «Orden europea de entrega»: decisión vinculante adoptada por una autoridad emisora de un Estado miembro que obligue a un proveedor que ofrezca servicios en la Unión y esté establecido o representado en el territorio de otro Estado miembro a entregar pruebas electrónicas.

(1) «Orden europea de conservación»: decisión vinculante adoptada por una autoridad emisora de un Estado miembro que obligue a un proveedor que ofrezca servicios en la Unión y esté establecido o representado en el territorio de otro Estado miembro a conservar pruebas electrónicas a efectos de una solicitud de entrega subsiguiente.

(2) «Proveedor de servicios»: persona física o jurídica que presta uno o más de los tipos de servicios siguientes:

   (a) servicios de comunicaciones electrónicas, según se definen en el artículo 2, apartado 4, de la [Directiva por la que se establece el Código Europeo de Comunicaciones Electrónicas];

   (b) servicios de la sociedad de la información, según se definen en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo[44], que cuenten con el almacenamiento de datos como componente esencial del servicio prestado al usuario, en particular las redes sociales, los mercados en línea que faciliten transacciones entre sus usuarios, y otros servicios de alojamiento de datos;

[44] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, DO L 241 de 17.9.2015, p. 1.

(c) servicios de asignación de nombres de dominio de internet y de direcciones IP, tales como proveedores de direcciones IP y registradores de nombres de dominio, así como servicios de privacidad y representación relacionados.

(3) «Ofrecer servicios en la Unión»:

(a) permitir que personas físicas o jurídicas en uno o más Estados miembros utilicen los servicios a los que se refiere el punto 3); y

(b) tener una estrecha vinculación con los Estados miembros a que se refiere la letra a).

(4) «Establecimiento»: ejercicio efectivo de una actividad económica por tiempo indefinido a través de una infraestructura estable a partir de la cual se realiza la actividad de prestación de servicios o de una infraestructura estable a partir de la cual se gestiona la actividad.

(5) «Pruebas electrónicas»: pruebas almacenadas en formato electrónico por un proveedor de servicios o en nombre del mismo en el momento de la recepción de un certificado de orden europea de entrega o de un certificado de orden europea de conservación, consistentes en datos de los abonados, datos relativos al acceso, datos de transacciones y datos de contenido almacenados.

(6) «Datos de los abonados»: cualquier dato en relación con:

(a) la identidad del abonado o cliente, como nombre, fecha de nacimiento, dirección postal o geográfica, facturación y pagos, teléfono o dirección de correo electrónico;

(b) el tipo de servicio y su duración, incluidos los datos técnicos que identifiquen las medidas técnicas correspondientes o las interfaces, utilizadas o facilitadas al abonado o cliente, y los datos relativos a la validación del uso del servicio, excluyendo las contraseñas u otros medios de autentificación utilizados en lugar de una contraseña que hayan sido facilitados por el usuario o creados a petición del usuario.

(7) «Datos relativos al acceso»: datos relativos al inicio y final de una sesión de acceso del usuario a un servicio, que sean estrictamente necesarios con el único fin de identificar al usuario del servicio, tales como la fecha y hora del acceso, o de conexión y desconexión al servicio, junto con la dirección IP asignada al usuario por el proveedor de servicios de acceso a internet, los datos identificativos de la interfaz utilizada y la identificación del usuario. Esto incluye los metadatos de comunicaciones electrónicas según se definen en el artículo 4, apartado 3, letra g), del [Reglamento relativo al respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas].

(8) «Datos de transacciones»: datos sobre transacciones relacionadas con la prestación de un servicio ofrecido por un proveedor de servicios que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del proveedor de servicios, tales como el origen y destino de un mensaje u otro tipo de interacción, la ubicación del dispositivo, la fecha, la hora, la duración, el tamaño, la ruta, el formato, el protocolo utilizado y el tipo de compresión, a menos que estos datos constituyan datos relativos al acceso. Se incluyen aquí los metadatos de las comunicaciones electrónicas, según se definen en el artículo 4, apartado 3, letra g), del [Reglamento relativo al respeto de la vida

privada y la protección de los datos personales en el sector de las comunicaciones electrónicas].

(9) «Datos de contenido»: todo dato almacenado en formato digital, como texto, voz, vídeos, imágenes y sonidos, distintos de los datos de los abonados, los datos relativos al acceso o los datos de transacciones.

(10) «Sistema de información»: sistema de información según lo definido en el artículo 2, letra a), de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo[45].

(11) «Estado emisor»: Estado miembro en el que se emita una orden europea de entrega o una orden europea de conservación.

(12) «Estado de ejecución»: Estado miembro en el que resida o tenga su sede el destinatario de una orden europea de entrega o de una orden europea de conservación o al que se transmita una orden europea de entrega y un certificado de orden europea de entrega o una orden europea de conservación y un certificado de orden europea de conservación a efectos de su ejecución.

(13) «Autoridad de ejecución»: autoridad competente del Estado de ejecución a la que la autoridad emisora transmita una orden europea de entrega o una orden europea de conservación a efectos de su ejecución.

(14) «Casos urgentes»: situaciones en las que exista una amenaza inminente para la vida o la integridad física de una persona o para una infraestructura esencial, tal como se define en el artículo 2, letra a), de la Directiva 2008/114/CE del Consejo[46].

Artículo 3
Ámbito de aplicación

1. El presente Reglamento se aplicará a los proveedores que ofrezcan servicios en la Unión.

2. Una orden europea de entrega o una orden europea de conservación solo podrá emitirse para procesos penales, tanto durante las fases previas al juicio como durante la fase procesal. Las órdenes también podrán ser emitidas en procesos relativos a infracciones penales por las que una persona jurídica pueda ser considerada responsable o ser castigada en el Estado emisor.

3. Las órdenes previstas por el presente Reglamento solo se podrán emitir para datos relativos a servicios ofrecidos en la Unión tal como se definen en el artículo 2, apartado 3.

---

45 Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, DO L 218 de 14.8.2013, p. 8).

46 Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, DO L 345 de 23.12.2008. p. 75

Capítulo 2: Orden europea de entrega, orden europea de conservación y certificados

Artículo 4
Autoridad emisora

1. Una orden europea de entrega relativa a datos de los abonados y datos relativos al acceso podrá ser emitida por:

   (a) un juez, tribunal, juez de instrucción o fiscal competentes en el asunto de que se trate; o

   (b) cualquier otra autoridad competente, según la defina el Estado emisor, que, en el asunto específico de que se trate, actúe en calidad de autoridad de investigación en procesos penales y tenga competencia para ordenar la obtención de pruebas con arreglo a la legislación nacional. La orden europea de entrega será validada previo examen de su cumplimiento de las condiciones de emisión en virtud del presente Reglamento, por un juez, tribunal, juez de instrucción o fiscal del Estado emisor.

2. Una orden europea de entrega relativa a datos de transacciones y datos de contenido solo podrá ser emitida por:

   (a) un juez, tribunal o juez de instrucción competente en el asunto de que se trate; o

   (b) cualquier otra autoridad competente, según la defina el Estado emisor que, en el asunto específico de que se trate, actúe en calidad de autoridad de investigación en procesos penales y tenga competencia para ordenar la obtención de pruebas con arreglo a la legislación nacional. La orden europea de entrega será validada previo examen de su cumplimiento de las condiciones de emisión en virtud del presente Reglamento, por un juez, tribunal o juez de instrucción del Estado emisor.

3. Una orden europea de conservación podrá ser emitida por:

   (a) un juez, tribunal, juez de instrucción o fiscal competentes en el asunto de que se trate; o

   (b) cualquier otra autoridad competente, según la defina el Estado emisor, que, en el asunto específico de que se trate, actúe en calidad de autoridad de investigación en procesos penales y tenga competencia para ordenar la obtención de pruebas con arreglo a la legislación nacional. La orden europea de conservación será validada, previo examen de su cumplimiento de las condiciones de emisión en virtud del presente Reglamento, por un juez, tribunal, juez de instrucción o fiscal del Estado emisor.

4. Cuando la orden haya sido validada por una autoridad judicial con arreglo al apartado 1, letra b), el apartado 2, letra b), y el apartado 3, letra b), dicha autoridad también podrá considerarse como una autoridad emisora a efectos de la transmisión del certificado de orden europea de entrega y del certificado de orden europea de conservación.

Artículo 5

Condiciones para la emisión de una orden europea de entrega

1. La autoridad emisora solo podrá emitir una orden europea de entrega cuando se cumplan las condiciones establecidas en el presente artículo.

2. La orden europea de entrega deberá ser necesaria y proporcionada a efectos de los procesos a que se refiere el artículo 3, apartado 2, y solo podrá emitirse si en el Estado emisor está prevista una medida similar para la misma infracción penal en una situación nacional comparable.

3. Podrá emitirse una orden europea de entrega con respecto a datos de los abonados o datos relativos al acceso para todas las infracciones penales.

4. Solo podrá emitirse una orden europea de entrega con respecto a datos de transacciones o datos relativos al acceso para:

   (a) infracciones penales punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años; o

   (b) las siguientes infracciones penales, siempre que hayan sido cometidas total o parcialmente por medio de un sistema de información:

   – las definidas en los artículos 3, 4 y 5 de la Decisión marco 2001/413/JAI del Consejo[47];

   – las definidas en los artículos 3 a 7 de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo[48];

   – las definidas en los artículos 3 a 8 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo;

   (c) las infracciones penales definidas en los artículo 3 a 12 y 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo[49].

5. La orden europea de entrega deberá incluir la información siguiente:

   (a) la autoridad emisora y, cuando proceda, la autoridad validadora;

   (b) el destinatario de la orden europea de entrega a que se refiere el artículo 7;

   (c) las personas cuyos datos se hayan solicitado, excepto cuando la única finalidad de la orden sea identificar a una persona;

   (d) la categoría de los datos solicitados (datos de los abonados, datos relativos al acceso, datos de transacciones o datos de contenido);

   (e) en su caso, el periodo que abarca la solicitud de entrega;

   (f) las disposiciones de Derecho penal aplicables del Estado emisor;

---

47 Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, DO L 149 de 2.6.2001, p. 1).

48 Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo, DO L 335 de 17.12.2011, p. 1).

49 Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo, DO L 88 de 31.3.2017, p. 6).

(g) en caso urgente o de petición de revelación rápida de la información, las razones que lo justifiquen;

(h) en los casos en que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa u otra entidad distinta de una persona física, confirmación de que la orden se solicita de conformidad con el apartado 6;

(i) la justificación de la necesidad y proporcionalidad de la medida.

6. En los casos en que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una empresa u otra entidad distinta de una persona física, la orden europea de entrega solo podrá remitirse al proveedor de servicios cuando no sean apropiadas medidas de investigación remitidas a la empresa o la entidad porque podrían poner en peligro la investigación.

7. En caso de que la autoridad emisora tenga motivos para creer que los datos de transacciones o los datos de contenido solicitados están protegidos por privilegios e inmunidades concedidos en virtud de la legislación del Estado miembro en el que reside o está establecido el proveedor de servicios, o que su revelación puede afectar a intereses fundamentales de dicho Estado miembro como la seguridad y la defensa nacionales, la autoridad emisora deberá pedir aclaraciones antes de emitir la orden europea de entrega, incluso mediante consulta a las autoridades competentes del Estado miembro de que se trate, bien directamente o bien a través de Eurojust o de la Red Judicial Europea. Si la autoridad emisora considera que los datos relativos al acceso, los datos de transacciones o los datos de contenido solicitados están protegidos por tales privilegios e inmunidades, o que su revelación afectaría a los intereses fundamentales del otro Estado miembro, no emitirá la orden europea de entrega.

Artículo 6

Condiciones para la emisión de una orden europea de conservación

1. La autoridad emisora solo podrá emitir una orden europea de conservación cuando se cumplan las condiciones establecidas en el presente artículo.

2. La orden podrá emitirse cuando sea necesaria y proporcionada para impedir la retirada, supresión o alteración de datos con vistas a una posterior solicitud de entrega de estos datos a través de la asistencia judicial mutua, una orden europea de investigación o una orden europea de entrega. Las órdenes europeas de conservación podrán emitirse para todas las infracciones penales.

3. La orden europea de conservación deberá incluir la información siguiente:

(a) la autoridad emisora y, cuando proceda, la autoridad validadora;

(b) el destinatario de la orden europea de conservación a que se refiere el artículo 7;

(c) las personas cuyos datos deban ser conservados, excepto cuando la única finalidad de la orden sea identificar a una persona;

(d) la categoría de los datos que deban ser conservados (datos de los abonados, datos relativos al acceso, datos de transacciones o datos de contenido);

(e) en su caso, el periodo que abarque la solicitud de conservación;

(f) las disposiciones de Derecho penal aplicables del Estado emisor;

(g) la justificación de la necesidad y proporcionalidad de la medida.

Artículo 7

Destinatario de la orden europea de entrega y de la orden europea de conservación

1. La orden europea de entrega y la orden europea de conservación deberán remitirse directamente al representante legal designado por el proveedor de servicios a efectos de recabar pruebas para procesos penales.

2. Si no se ha designado un representante legal específico, la orden europea de entrega y la orden europea de conservación podrán remitirse a cualquier establecimiento del proveedor en la Unión.

3. En caso de que el representante legal no cumpla una orden europea de entrega en un caso urgente con arreglo al artículo 9, apartado 2, la orden podrá remitirse a cualquier establecimiento del proveedor en la Unión.

4. En caso de que el representante legal no cumpla las obligaciones que le incumben en virtud de los artículos 9 o 10 y la autoridad emisora considere que existe un riesgo grave de pérdida de datos, la orden europea de entrega o la orden europea de conservación podrán remitirse a cualquier establecimiento del proveedor en la Unión.

Artículo 8

Certificado de orden europea de entrega y certificado de orden europea de conservación

1. La orden europea de entrega o la orden europea de conservación se transmitirán al destinatario, tal como se define en el artículo 7, a través de un certificado de orden europea de entrega (en lo sucesivo, «EPOC», por sus siglas en inglés) o de un certificado de orden europea de conservación (en lo sucesivo, «EPOC-PR», por sus siglas en inglés).

   La autoridad emisora o la autoridad validadora completarán el EPOC establecido en el anexo I o el EPOC-PR establecido en el anexo II, certificarán su contenido como exacto y correcto, y lo firmarán.

2. El EPOC y el EPOC-PR deberán ser transmitidos directamente por cualquier medio que pueda dejar constancia escrita en condiciones que permitan al destinatario determinar su autenticidad.

   En caso de que los proveedores de servicios, los Estados miembros o los organismos de la Unión hayan establecido plataformas especializadas u otros canales seguros para la tramitación de las solicitudes de datos por las autoridades policiales y judiciales, la autoridad emisora también podrá optar por transmitir el certificado a través de estos canales.

3. El EPOC deberá contener la información mencionada en el artículo 5, apartado 5, letras a) a h), e incluir datos suficientes que permitan al destinatario identificar y ponerse en contacto con la autoridad emisora. No deberán incluirse la justificación de la necesidad y la proporcionalidad de la medida ni precisiones adicionales sobre las investigaciones.

4. El EPOC-PR deberá contener la información mencionada en el artículo 6, apartado 3, letras a) a f), e incluir datos suficientes que permitan al destinatario identificar y ponerse en contacto con la autoridad emisora. No deberán incluirse la justificación de

la necesidad y la proporcionalidad de la medida ni precisiones adicionales sobre las investigaciones.

5. En caso necesario, el EPOC o el EPCO-PR se traducirán a una lengua oficial de la Unión aceptada por el destinatario. En caso de que no se haya especificado ninguna lengua, se traducirán a una de las lenguas oficiales del Estado miembro en el que resida o esté establecido el representante legal.

Artículo 9
Ejecución del EPOC

1. Una vez recibido el EPOC, el destinatario velará por que los datos solicitados se transmitan directamente a la autoridad emisora o a las autoridades policiales o judiciales indicadas en el EPOC a más tardar en el plazo de 10 días desde la recepción del mismo, salvo si la autoridad emisora indica razones para una revelación más rápida.

2. En casos urgentes, el destinatario remitirá los datos solicitados sin demora, a más tardar en un plazo de seis horas tras la recepción del EPOC.

3. En caso de que no pueda cumplir su obligación porque el EPOC esté incompleto, contenga errores manifiestos o no contenga información suficiente para ejecutarlo, el destinatario informará a la autoridad emisora indicada en el EPOC, sin demora indebida, y solicitará aclaraciones utilizando el formulario que figura en el anexo III. Informará a la autoridad emisora sobre si fue posible una identificación y conservación, tal como se establece en el apartado 6. La autoridad emisora responderá sin demora y en un plazo máximo de cinco días. Los plazos establecidos en los apartados 1 y 2 no se aplicarán hasta que se hayan facilitado las aclaraciones pertinentes.

4. Si el destinatario no pudiera cumplir sus obligaciones por causa de fuerza mayor o imposibilidad material no imputable a él o, en su caso, al proveedor de servicios, en particular porque la persona cuyos datos se solicitan no sea su cliente o porque los datos se hayan suprimido antes de recibir el EPOC, el destinatario informará a la autoridad emisora citada en el EPOC sin demora indebida explicando las razones, mediante el formulario que figura en el anexo III. Si se cumplen las condiciones pertinentes, la autoridad emisora retirará el EPOC.

5. En todos los casos en que, por otros motivos, el destinatario no aporte la información solicitada o no la facilite de forma exhaustiva o en el plazo establecido, informará de ello a la autoridad emisora sin demora injustificada, y a más tardar en los plazos establecidos en los apartados 1 y 2, explicando los motivos de la utilización del formulario que figura en el anexo III. La autoridad competente del Estado emisor examinará la orden a la luz de la información facilitada por el proveedor de servicios y, si procede, fijará un nuevo plazo para que el proveedor de servicios entregue los datos.

   En caso de que el destinatario entienda que el EPOC no puede ejecutarse porque, basándose únicamente en la información en él contenida, se desprenda que es claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea o manifiestamente abusivo, deberá asimismo enviar el formulario que figura en el anexo III a la autoridad de ejecución competente de su propio Estado miembro. En tales casos, la autoridad de ejecución competente podrá solicitar aclaraciones a la

autoridad emisora sobre la orden europea de entrega, bien directamente o a través de Eurojust o de la Red Judicial Europea.

6. Si no entrega inmediatamente los datos solicitados, el destinatario deberá conservarlos, salvo que la información contenida en el EPOC no le permita identificar los datos solicitados, en cuyo caso deberá solicitar aclaraciones de conformidad con el apartado 3. Los datos deberán conservarse hasta su entrega en virtud de la orden europea de entrega con sus aclaraciones y del correspondiente certificado, o a través de otros canales, como la asistencia judicial mutua. En caso de que la entrega y la conservación de los datos ya no sean necesarias, la autoridad competente del Estado emisor y, cuando proceda de conformidad con el artículo 14, apartado 8, la autoridad de ejecución, informará al destinatario sin demora indebida.

Artículo 10
Ejecución del EPOC-PR

1. Una vez recibido el EPOC-PR, el destinatario deberá conservar, sin demora injustificada, los datos solicitados. La conservación expirará transcurridos 60 días, a menos que la autoridad emisora confirme que se ha puesto en marcha la subsiguiente solicitud de entrega.

2. En caso de que la autoridad emisora confirme en el plazo establecido en el apartado 1 que se ha puesto en marcha la solicitud de entrega, el destinatario deberá conservar los datos durante el tiempo necesario para entregarlos una vez que la solicitud subsiguiente de entrega haya sido notificada.

3. En caso de que la conservación ya no sea necesaria, la autoridad emisora informará al destinatario sin demora indebida.

4. En caso de que no pueda cumplir su obligación porque el certificado esté incompleto, contenga errores manifiestos o no contenga información suficiente para ejecutarlo, el destinatario informará a la autoridad emisora indicada en el EPOC-PR, sin demora indebida, y solicitará aclaraciones utilizando el formulario que figura en el anexo III. La autoridad emisora responderá sin demora y en un plazo máximo de cinco días. El destinatario garantizará, por su parte, que está en condiciones de recibir las aclaraciones necesarias para cumplir la obligación contemplada en el apartado 1.

5. Si el destinatario no pudiera cumplir sus obligaciones por causa de fuerza mayor o imposibilidad material no imputable a él o, en su caso, al proveedor de servicios, en particular porque la persona cuyos datos se solicitan no sea su cliente o porque los datos se hayan suprimido antes de recibir la orden, el destinatario informará a la autoridad emisora citada en el EPOC-PR sin demora indebida explicando las razones, mediante el formulario que figura en el anexo III. Si se cumplen estas condiciones, la autoridad emisora retirará el EPOC-PR.

6. En todos los casos en que, por otros motivos indicados en el formulario del anexo III, no conserve la información solicitada, el destinatario comunicará los motivos a la autoridad emisora sin demora, utilizando el formulario que figura en el anexo III. La autoridad emisora examinará la orden a la luz de la justificación alegada por el proveedor de servicios.

Artículo 11
Confidencialidad e información al usuario

1. El destinatario, y en su caso el proveedor de servicios, adoptará las medidas necesarias para garantizar la confidencialidad del EPOC o del EPOC-PR y de los datos entregados o conservados, y si así lo solicita la autoridad emisora, se abstendrá de informar a la persona cuyos datos se buscan con objeto de no obstruir el proceso penal pertinente.
2. Cuando solicite al destinatario que se abstenga de informar a la persona cuyos datos se buscan a través del EPOC, la autoridad emisora informará sin demora injustificada a dicha persona de la entrega de los datos. Esta información podrá aplazarse el tiempo que sea necesario y proporcionado con objeto de no obstruir el proceso penal pertinente.
3. Al informar a la persona, la autoridad emisora deberá incluir información sobre las vías de recurso disponibles a que se refiere el artículo 17.

Artículo 12
Reembolso de gastos

Siempre que se contemple en la legislación nacional del Estado emisor con respecto a órdenes nacionales en situaciones similares, el proveedor de servicios podrá reclamar el reembolso de los gastos al Estado emisor, con arreglo a dichas disposiciones nacionales.

Capítulo 3: Sanciones y ejecución

Artículo 13
Sanciones

Sin perjuicio de lo dispuesto en las legislaciones nacionales que prevean la imposición de sanciones penales, los Estados miembros establecerán normas relativas a las sanciones pecuniarias aplicables en caso de incumplimiento de las obligaciones previstas en los artículos 9, 10 y 11 del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Las sanciones pecuniarias deberán ser eficaces, proporcionadas y disuasorias. Los Estados miembros notificarán sin demora a la Comisión dichas normas y medidas, así como cualquier modificación posterior de las mismas.

Artículo 14
Procedimiento de ejecución

1. En caso de que el destinatario no cumpla un EPOC en el plazo establecido o un EPOC-PR sin aportar razones aceptadas por la autoridad emisora, esta podrá trasladar a la autoridad competente del Estado de ejecución la orden europea de entrega con el EPOC o la orden europea de conservación con el EPOC-PR, así como el formulario que figura en el anexo III cumplimentado por el destinatario y cualquier otro documento pertinente, con vistas a su ejecución por cualquier medio que pueda dejar constancia escrita en condiciones que permitan a la autoridad de ejecución establecer su autenticidad. A tal efecto, la autoridad emisora traducirá la orden, el formulario y la documentación adjunta a una de las lenguas oficiales de tal Estado miembro, e informará al destinatario del traslado.

2. Una vez recibida la documentación, la autoridad de ejecución reconocerá sin más trámites la orden europea de entrega o la orden europea de conservación transmitidas de conformidad con el apartado 1 y tomará las medidas necesarias para su ejecución, salvo que la autoridad de ejecución considere que es aplicable alguno de los motivos previstos en los apartados 4 o 5 o que los datos en cuestión están protegidos por privilegios o inmunidades con arreglo a su legislación nacional o que su revelación puede afectar a sus intereses fundamentales, como la seguridad y la defensa nacionales. La autoridad de ejecución adoptará la decisión de reconocimiento de la orden sin demora indebida y, a más tardar, cinco días hábiles después de la recepción de la misma.

3. Cuando la autoridad de ejecución reconozca la orden, requerirá formalmente al destinatario para que cumpla la obligación pertinente, informándole de la posibilidad de oponerse a la ejecución alegando los motivos enumerados en los apartados 4 o 5, así como de las sanciones aplicables en caso de incumplimiento, y establecerá un plazo para dar cumplimiento o manifestar la oposición.

4. El destinatario solo podrá oponerse a la ejecución de la orden europea de entrega por los motivos siguientes:

   (a) la orden europea de entrega no ha sido emitida o validada por una autoridad emisora con arreglo a lo dispuesto en el artículo 4;

   (b) la orden europea de entrega no ha sido emitida respecto de una infracción prevista en el artículo 5, apartado 4;

   (c) el destinatario no pudo ejecutar el EPOC por imposibilidad material o fuerza mayor, o porque el EPOC contiene errores manifiestos;

   (d) la orden europea de entrega no se refiere a datos almacenados por el proveedor de servicios, o en su nombre, en el momento de la recepción del EPOC;

   (e) el servicio no está cubierto por el presente Reglamento;

   (f) basándose únicamente en la información contenida en el EPOC, se desprende que es claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea o manifiestamente abusivo.

5. El destinatario solo podrá oponerse a la ejecución de la orden europea de conservación por los motivos siguientes:

   (a) la orden europea de conservación no ha sido emitida o validada por una autoridad emisora con arreglo a lo dispuesto en el artículo 4;

   (b) el proveedor de servicios no pudo ejecutar el EPOC-PR por imposibilidad material o fuerza mayor, o porque el EPOC-PR contiene errores manifiestos;

   (c) la orden europea de conservación no se refiere a datos almacenados por el proveedor de servicios, o en su nombre, en el momento de la recepción del EPOC-PR;

   (d) el servicio no está cubierto por el presente Reglamento;

   (e) basándose únicamente en la información contenida en el EPOC-PR, se desprende que es claramente contrario a la Carta de los Derechos Fundamentales de la Unión Europea o manifiestamente abusivo.

6. En caso de oposición del destinatario, la autoridad de ejecución decidirá si ejecuta o no la orden sobre la base de la información facilitada por el destinatario y, en su

caso, de la información adicional obtenida de la autoridad emisora de conformidad con el apartado 7.

7. Antes de decidir no reconocer o ejecutar la orden con arreglo a lo dispuesto en los apartados 2 y 6, la autoridad de ejecución consultará a la autoridad emisora por cualquier medio que considere adecuado. En su caso, podrá solicitar información adicional a la autoridad emisora. La autoridad emisora responderá a tal solicitud en un plazo de cinco días hábiles.

8. Todas las decisiones se notificarán inmediatamente a la autoridad emisora, así como al destinatario, por cualquier medio que pueda dejar constancia escrita.

9. En caso de que la autoridad de ejecución obtenga los datos del destinatario, los transmitirá a la autoridad emisora en el plazo de dos días hábiles, a no ser que los datos en cuestión estén protegidos por un privilegio o inmunidad en virtud de su propio Derecho interno o que afecten a intereses fundamentales, como la seguridad y la defensa nacionales. En tal caso, informará a la autoridad emisora acerca de los motivos de la no transmisión de los datos.

10. En caso de que el destinatario no cumpla las obligaciones que le incumben en virtud de una orden reconocida cuya aplicabilidad haya sido confirmada por la autoridad de ejecución, dicha autoridad podrá imponer una sanción pecuniaria de conformidad con su legislación nacional. Contra la decisión que impone la sanción existe un recurso judicial efectivo.

Capítulo 4: Vías de recurso

Artículo 15

Procedimiento de reexamen en caso de obligaciones contradictorias basadas en derechos fundamentales o en intereses fundamentales de un país tercero

1. En caso de que el destinatario considere que la ejecución de la orden europea de entrega entraría en conflicto con la legislación aplicable de un país tercero que prohíba la revelación de los datos en cuestión por la necesidad de proteger los derechos fundamentales de las personas interesadas o intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, informará a la autoridad emisora de sus motivos para no ejecutar la orden europea de entrega, de acuerdo con el procedimiento a que se refiere el artículo 9, apartado 5.

2. La oposición motivada contendrá toda la información pertinente sobre la legislación del país tercero, su aplicabilidad al caso en cuestión y la naturaleza de la obligación contradictoria. No podrá basarse en la ausencia, en la legislación aplicable del país tercero, de disposiciones similares relativas a las condiciones, formalidades y procedimientos de emisión de una orden de entrega, ni en la única circunstancia de que los datos se almacenen en un país tercero.

3. La autoridad competente del Estado emisor examinará la orden europea de entrega sobre la base de la objeción motivada. Si pretende confirmarla, deberá solicitar una revisión por el órgano jurisdiccional competente del propio Estado miembro. La ejecución de la orden se suspenderá a la espera de que concluya el procedimiento de revisión.

El órgano jurisdiccional competente deberá evaluar en primer lugar si existe un conflicto, examinando:

(a) si, con arreglo a las circunstancias específicas del caso en cuestión, es aplicable la legislación del país tercero, y en caso afirmativo,

(b) si la legislación del país tercero, aplicada a las circunstancias concretas del caso, prohíbe la revelación de los datos en cuestión.

4. Al proceder a esta apreciación, el órgano jurisdiccional deberá tener en cuenta si la legislación del país tercero, en lugar de proteger los derechos fundamentales o los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales, pretende manifiestamente proteger otros intereses o tiene como objetivo proteger actividades ilegales frente a requerimientos de las autoridades policiales o judiciales en el contexto de investigaciones penales.

5. En caso de que el órgano jurisdiccional competente considere que no existe conflicto en el sentido de los apartados 1 y 4, confirmará la orden. Si comprueba la existencia de un conflicto en el sentido de los apartados 1 y 4, transmitirá todos los elementos de hecho y de Derecho pertinentes en relación con el asunto, así como su evaluación, a las autoridades centrales del país tercero de que se trate, a través de su autoridad central nacional, fijando un plazo de 15 días para que dichas autoridades respondan. Previa solicitud motivada de la autoridad central del país tercero, el plazo podrá ser prorrogado por 30 días.

6. En caso de que, en el plazo fijado, la autoridad central del país tercero comunique al órgano jurisdiccional competente que se opone a la ejecución de la orden europea de entrega en el caso de autos, el órgano jurisdiccional competente anulará la orden e informará de ello a la autoridad emisora y al destinatario. En caso de que no se reciba objeción alguna en el plazo fijado (en su caso, prorrogado), el órgano jurisdiccional competente enviará un recordatorio a la autoridad central del país tercero concediéndole un plazo suplementario de cinco días para responder e informándole de las consecuencias de la falta de respuesta. En caso de que no se reciba objeción alguna en dicho plazo adicional, el órgano jurisdiccional competente confirmará la orden.

7. En caso de que el órgano jurisdiccional competente determine que la orden debe confirmarse, informará de ello a la autoridad emisora y al destinatario, que deberá ejecutar la orden.

Artículo 16

Procedimiento de reexamen en caso de obligaciones contradictorias basadas en otros motivos

1. En caso de que el destinatario considere que la ejecución de la orden europea de entrega entraría en conflicto con la legislación aplicable de un país tercero que prohíba la revelación de los datos en cuestión por razones distintas de las contempladas en el artículo 15, informará a la autoridad emisora de sus motivos para no ejecutar la orden europea de entrega, con arreglo al procedimiento descrito en el artículo 9, apartado 5.

2. La objeción motivada deberá contener todos los detalles pertinentes sobre la legislación del país tercero, su aplicabilidad al caso de autos y la naturaleza de la obligación contradictoria. No podrá basarse en el hecho de que en la legislación aplicable del país tercero no existan disposiciones similares relativas a las

condiciones, las formalidades y los procedimientos de emisión de una orden de entrega, ni en la única circunstancia de que los datos se almacenen en un país tercero.

3. La autoridad emisora examinará la orden europea de entrega sobre la base de la objeción motivada. Si la autoridad emisora pretende confirmar la orden europea de entrega, solicitará una revisión por el tribunal competente de su Estado miembro. La ejecución de la orden se suspenderá a la espera de que concluya el procedimiento de revisión.

4. El órgano jurisdiccional competente deberá evaluar en primer lugar si existe un conflicto, examinando si:

es aplicable la legislación del país tercero, según las circunstancias específicas del caso de que se trate y, en caso afirmativo,

(a) la legislación del país tercero, aplicada a las circunstancias concretas del caso de que se trate, prohíbe la revelación de los datos en cuestión.

5. En caso de que el órgano jurisdiccional competente considere que no existe un conflicto relevante en el sentido de los apartados 1 y 4, deberá confirmar la orden. En caso de que el órgano jurisdiccional competente compruebe que la legislación de un país tercero, cuando se aplica a las circunstancias concretas del caso de autos, prohíbe la revelación de los datos en cuestión, determinará si confirma o retira la orden, basándose en particular en los siguientes elementos:

(a) el interés protegido por la legislación pertinente del país tercero, incluido el interés del país tercero en impedir la revelación de los datos;

(b) el grado de vinculación de la causa penal para la que se haya emitido la orden con cualquiera de las dos jurisdicciones, resultante, entre otros:

- de la ubicación, la nacionalidad y el lugar de residencia de la persona cuyos datos se solicitan, o de la víctima;

- del lugar en el que se haya cometido el delito en cuestión;

(c) el grado de vinculación entre el proveedor de servicios y el país tercero en cuestión; en este contexto, el lugar de almacenamiento de los datos en sí no es suficiente para establecer un grado de vinculación significativo;

(d) los intereses del Estado investigador en la obtención de las pruebas en cuestión, en función de la gravedad de la infracción y la importancia de la obtención de pruebas con prontitud;

(e) las posibles consecuencias para el destinatario o el proveedor de servicios de cumplir la orden europea de entrega, incluidas las sanciones que puedan aplicarse.

6. En caso de que el órgano jurisdiccional competente decida anular la orden, informará de ello a la autoridad emisora y al destinatario. En caso de que el órgano jurisdiccional competente determine que la orden debe mantenerse, informará de ello a la autoridad emisora y al destinatario, que procederá a ejecutar la orden.

Artículo 17
Vías de recurso efectivas

1. Los sospechosos o acusados cuyos datos hayan sido obtenidos mediante una orden europea de entrega tendrán derecho a vías de recurso efectivas contra dicha orden durante el proceso penal para el que se haya emitido la orden, sin perjuicio de las vías de recurso disponibles con arreglo a la Directiva (UE) 2016/680 y al Reglamento (UE) 2016/679.
2. Cuando la persona cuyos datos se hayan obtenido no sea un sospechoso o acusado en un proceso penal para el que se haya emitido la orden, dicha persona tendrá derecho a vías de recurso efectivas contra una orden europea de entrega en el Estado emisor, sin perjuicio de las vías de recurso disponibles con arreglo a la Directiva (UE) 2016/680 y al Reglamento (UE) 2016/679.
3. Este derecho a una tutela judicial efectiva se ejercerá ante un órgano jurisdiccional en el Estado emisor con arreglo a su legislación nacional y deberá incluir la posibilidad de impugnar la legalidad, la necesidad y la proporcionalidad de la medida.
4. Sin perjuicio de lo dispuesto en el artículo 11, la autoridad emisora tomará las medidas adecuadas para garantizar que se facilite información sobre las posibilidades de recurso, de conformidad con la legislación nacional, y para garantizar su ejercicio efectivo.
5. Los plazos u otras condiciones para la interposición de un recurso serán iguales a los previstos en casos internos similares y se aplicarán de modo que se garantice a las personas afectadas el ejercicio efectivo del recurso.
6. Sin perjuicio de las normas procesales nacionales, los Estados miembros velarán por que, en los procesos penales en el Estado emisor, se respeten los derechos de la defensa y la equidad del proceso al evaluar las pruebas obtenidas a través de la orden europea de entrega.

Artículo 18
Respeto de los privilegios e inmunidades en virtud de la legislación del Estado de ejecución

En caso de que los datos de transacciones o los datos de contenido obtenidos a través de la orden europea de entrega estén protegidos por privilegios o inmunidades concedidos en virtud de la legislación del Estado miembro del destinatario, o afecten a intereses fundamentales de dicho Estado miembro, como la seguridad y la defensa nacionales, el órgano jurisdiccional del Estado emisor garantizará durante el proceso penal para el que se haya emitido la orden que esos motivos sean tenidos en cuenta en las mismas condiciones que si estuvieran previstos por su legislación nacional, al evaluar la pertinencia y la admisibilidad de las pruebas en cuestión. El órgano jurisdiccional podrá consultar a las autoridades del Estado miembro de que se trate, a la Red Judicial Europea en materia penal o a Eurojust.

Capítulo 5: Disposiciones finales

Artículo 19
Seguimiento y presentación de informes

1. A más tardar el [*fecha de aplicación del presente Reglamento*], la Comisión elaborará un programa detallado para el seguimiento de los resultados y las

repercusiones del presente Reglamento. El programa deberá establecer las modalidades y la periodicidad de recopilación de los datos y demás pruebas necesarias, y especificará las medidas que deben adoptar la Comisión y los Estados miembros para recopilar y analizar los datos y otras pruebas.

2. En cualquier caso, los Estados miembros deberán recopilar y conservar estadísticas exhaustivas facilitadas por las autoridades pertinentes. Los datos recogidos se enviarán a la Comisión a más tardar el 31 de marzo de cada año para el año civil anterior, e incluirán:

   (a) el número de EPOC y EPOC-PR emitidos por tipo de datos solicitados, por proveedores de servicios destinatarios y por situación (desglose entre casos urgentes y no urgentes);

   (b) el número de EPOC ejecutados y no ejecutados por tipo de datos solicitados, por proveedores de servicios destinatarios y por situación (desglose entre casos urgentes y no urgentes);

   (c) para los EPOC ejecutados, la duración media para obtener los datos solicitados desde el momento de emisión de la orden europea de entrega hasta el momento en que se obtuvieron, por tipo de datos solicitados, por proveedores de servicios destinatarios y por situación (desglose entre casos urgentes y no urgentes);

   (d) el número de órdenes europeas de entrega transmitidas a un Estado de ejecución y recibidas para su ejecución, por tipo de datos solicitados, por proveedores de servicios destinatarios y por situación (desglose entre casos urgentes y no urgentes), y el número de dichas órdenes ejecutadas;

   (e) el número de recursos judiciales contra las órdenes europeas de entrega en el Estado emisor y en el Estado de ejecución por tipo de datos solicitados.

Artículo 20
Modificaciones de los certificados y formularios

La Comisión adoptará actos delegados de conformidad con el artículo 21 a fin de modificar los anexos I, II y III con objeto de abordar de forma efectiva la posible necesidad de mejoras en lo que concierne al contenido de los formularios de EPOC y de EPOC-PR y de los formularios que deben utilizarse para facilitar información sobre la imposibilidad de ejecutar un EPOC o un EPOC-PR.

Artículo 21
Ejercicio de la delegación

1. Se otorgan a la Comisión poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. La delegación de poderes a que se refiere el artículo 20 se otorgará por tiempo indefinido a partir del [*fecha de aplicación del presente Reglamento*].

3. La delegación de poderes mencionada en el artículo 20 podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de cualesquiera actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación, de 13 de abril de 2016[50].

5. Tan pronto como la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 20 entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo o al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no formularán objeciones. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 22
Notificaciones

1. A más tardar el [*fecha de aplicación del presente Reglamento*], cada Estado miembro notificará a la Comisión:

   (a) las autoridades que, con arreglo a su legislación nacional, son competentes de conformidad con lo dispuesto en el artículo 4 para emitir o validar órdenes europeas de entrega y órdenes europeas de conservación;

   (b) la autoridad o autoridades de ejecución competentes para ejecutar órdenes europeas de entrega y órdenes europeas de conservación en nombre de otro Estado miembro;

   (c) los órganos jurisdiccionales competentes para pronunciarse sobre las objeciones motivadas de los destinatarios de conformidad con los artículos 15 y 16.

2. La Comisión pondrá la información recibida en virtud del presente artículo a disposición del público, bien en un sitio web específico o en el sitio web de la Red Judicial Europea mencionado en el artículo 9 de la Decisión 2008/976/JAI del Consejo[51].

Artículo 23
Relación con las órdenes europeas de investigación

Las autoridades de los Estados miembros podrán continuar emitiendo órdenes europeas de investigación con arreglo a lo dispuesto en la Directiva 2014/41/UE para la obtención de pruebas que también estén contempladas en el ámbito de aplicación del presente Reglamento.

Artículo 24
Evaluación

A más tardar [*cinco años a partir de la fecha de aplicación del presente Reglamento*] la Comisión evaluará el presente Reglamento y presentará un informe al Parlamento Europeo y

[50] DO L 123 de 12.5.2016, p. 13.
[51] Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea, DO L 348 de 24.12.2008, p. 130.

al Consejo sobre el funcionamiento del mismo, incluyendo una evaluación de la necesidad de ampliar su alcance. En caso necesario, el informe irá acompañado de propuestas legislativas. La evaluación se efectuará con arreglo a las directrices de la Comisión para la mejora de la legislación. Los Estados miembros facilitarán a la Comisión la información necesaria para la preparación de dicho informe.

Artículo 25
Entrada en vigor

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del [*seis meses después de su entrada en vigor*].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en los Estados miembros de conformidad con los Tratados.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*