



Bruselas, 30 de noviembre de 2018
(OR. en)

15020/18

**Expediente interinstitucional:
2018/0108(COD)**

JAI 1236
COPEN 428
CYBER 304
DROIPEN 192
JAIEX 160
ENFOPOL 596
DAPIX 366
EJUSTICE 163
MI 917
TELECOM 442
DATAPROTECT 263
CODEC 2180

NOTA

| | |
|-----------------|---|
| De: | Presidencia |
| A: | Consejo |
| N.º doc. prec.: | 14351/1/18 REV1 |
| N.º doc. Ción.: | 8110/18 |
| Asunto: | Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal - Orientación general |

INTRODUCCIÓN

1. El 17 de abril de 2018, la Comisión adoptó y remitió al Consejo y al Parlamento Europeo la propuesta de referencia con el artículo 82, artículo 1, del TFUE como base jurídica. Tiene como objetivo crear órdenes europeas de «entrega» y «conservación» para conseguir o conservar pruebas electrónicas en otra jurisdicción sin la participación de las autoridades competentes en dicha jurisdicción. Las órdenes se refieren específicamente al acceso transfronterizo a las pruebas electrónicas, en un intento de adaptar los mecanismos de cooperación judicial a los requisitos de la lucha contra la delincuencia en la era digital.

2. El Reglamento propuesto establece la posibilidad de solicitar cualquier categoría de datos almacenados. Sin embargo, establece un umbral específico para los datos de tráfico y contenido [en contraposición a los datos de abonados y de acceso] que se pueden únicamente solicitar para delitos punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años o para delitos específicos relacionados con el ciberespacio o cometidos mediante la utilización del ciberespacio, o para delitos de terrorismo
3. La propuesta prevé un plazo obligatorio de diez días para la ejecución de la orden europea de entrega, pero en situaciones de urgencia (amenaza inminente para la vida o la integridad física de una persona o para una infraestructura esencial) el plazo es de seis horas. En cuanto a la orden europea de conservación, la autoridad competente tiene 60 días para confirmar que ha emitido la posterior solicitud de entrega de los datos (también mediante la asistencia judicial mutua). En caso de incumplimiento de una orden, se podrán imponer sanciones al proveedor de servicios.
4. Las órdenes se deben dirigir a un proveedor de servicios que ofrezca servicios en la Unión o a un representante legal designado por el proveedor de servicios, situado en otro Estado miembro, a efectos de recabar pruebas electrónicas de conformidad con la Directiva propuesta. El proyecto de Reglamento utiliza como criterio el tipo de servicios suministrados (comunicaciones electrónicas, servicios de la sociedad de la información, servicios de alojamiento, de direcciones IP, servicios de privacidad o de representación), pero también nombres de determinados tipos de proveedores de servicios (registros y registradores de nombres de dominio de internet).
5. El 18 de octubre de 2018, el Consejo Europeo¹ pidió soluciones para garantizar el acceso transfronterizo rápido y efectivo a las pruebas electrónicas, con objeto de combatir eficazmente el terrorismo y otras formas de delincuencia grave y organizada, tanto en la UE como a escala internacional. Subrayó que debía alcanzarse un acuerdo, a más tardar al final de la legislatura, sobre las propuestas de la Comisión relativas a las pruebas electrónicas.
6. En el Parlamento Europeo, D.^a Birgit Sippel (LIBE, S&D) fue nombrada ponente el 24 de mayo de 2018. La Comisión LIBE debatió la propuesta el 11 de junio de 2018 y ha mantenido varias reuniones y audiencias, en particular una audiencia pública el 27 de noviembre de 2018. No se ha establecido un plazo para la aprobación del informe.
7. El Comité Económico y Social aprobó su dictamen el 12 de julio de 2018².

¹ Doc. EUCO 13/18, apartado 9.

² Documento 11533/18.

II. TRABAJOS EN EL CONSEJO

8. La Comisión presentó esta propuesta al Grupo «Cooperación en Materia Penal» el 27 de abril de 2018, seguida de un examen artículo por artículo del proyecto de Reglamento y un cambio de impresiones sobre la evaluación de impacto que se mantuvo en el Grupo los días 5 y 6 de mayo de 2018. En general, las delegaciones acogieron positivamente la evaluación de impacto y la propuesta.
9. Los debates se centraron principalmente en torno al concepto propuesto por la Comisión de notificar una orden europea de entrega directamente al proveedor de servicios o a su representante legal sin la intervención del Estado miembro donde este último esté situado (es decir, el Estado de ejecución), la definición de proveedor de servicios, las inmunidades y privilegios, el procedimiento de reexamen en caso de obligaciones contradictorias y las sanciones por incumplimiento de las obligaciones derivadas del Reglamento.
10. El Grupo estudió la propuesta durante las Presidencias búlgara y austriaca. Se celebraron doce reuniones que resultaron en cinco versiones revisadas consecutivas. Los debates concluyeron el 20 de noviembre de 2018 con vistas a presentar el texto transaccional que figura en el anexo de la presente nota para su adopción como orientación general sobre la propuesta en el próximo Consejo JAI, que se celebrará el 6 y 7 de diciembre de 2018.
11. El resultado de los debates en las reuniones del Grupo, una vez recibidas por escrito las aportaciones de las delegaciones y las reservas de los Estados miembros sobre el texto, se refleja en el texto transaccional revisado de la Presidencia que figura en el anexo. Los considerandos se han adaptado a fin de reflejar los cambios introducidos en la parte dispositiva. Los cambios con respecto a la propuesta de la Comisión se indican en **negrita** (texto nuevo) o mediante el símbolo [...] (texto suprimido).

III. CONCLUSIÓN

12. El texto que figura en el anexo refleja los esfuerzos de la Presidencia y de los Estados miembros de llegar a un compromiso.
 13. El 28 de noviembre de 2018, el Comité de Representantes Permanentes alcanzó un acuerdo sobre el texto transaccional de la Presidencia que figura en el anexo de la presente nota, con el levantamiento de la reserva de la delegación SI en la nota al pie n.º 27 como única modificación.
 14. Se invita, por tanto, al Consejo a que adopte una orientación general sobre este texto, que constituirá la base para las negociaciones con el Parlamento Europeo en el marco del procedimiento legislativo ordinario (artículo 294 del TFUE).
-

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal³

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 Europeo⁴,

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 Países Bajos, Finlandia, República Checa y Letonia formulan una reserva sobre la totalidad del texto transaccional. En lo que respecta a los Países Bajos, dicha reserva se refiere, entre otros, a los artículos 5, 6, 7 *bis*, 11, apartado 3, 12 *bis*, 12 *ter*, 14 y 17.

⁴ DO C de , p. .

- (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 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 2017⁵, 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 2017⁶, 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.

⁵ JOIN(2017) 450 final.

⁶ Doc. 2017/2068(INI).

- (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 **sistemática** de un órgano judicial en el Estado miembro del proveedor del servicio **en cada caso**.
- (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.
- (12 bis) 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 Consejo⁷. En cualquier caso, no se debe emitir una orden europea de entrega, si el Estado miembro emisor tiene indicios de que hacerlo sería contrario al principio *ne bis in idem*.**

⁷ [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.

- (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/UE⁸, 2012/13/UE⁹, 2013/48/UE¹⁰, 2016/343¹¹, 2016/800¹² y 2016/1919¹³ del Parlamento Europeo y del Consejo.
- (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.

⁸ [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.

⁹ [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.

¹⁰ [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.

¹¹ [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.

¹² [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.

¹³ [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.

- (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. Se incluyen las comunicaciones interpersonales tales como los servicios de voz sobre IP, los servicios de mensajería instantánea y los servicios de correo electrónico. **El presente Reglamento debe aplicarse también a otros proveedores [...] de servicios de la sociedad de la información [...] en el sentido de la Directiva (UE) 2015/1535 [...] que no pueden calificarse como servicios de comunicaciones electrónicas, pero que ofrecen a sus usuarios la capacidad de comunicar entre sí o bien servicios que los usuarios pueden utilizar para tratar o almacenar datos. Ello debe adecuarse a los términos empleados en el Convenio de Budapest sobre la Ciberdelincuencia. El tratamiento de datos debe entenderse en un sentido técnico, como creación o manipulación de datos, es decir, operaciones técnicas destinadas a producir o modificar datos mediante la capacidad de procesamiento de un ordenador. Se trata de categorías de proveedores de servicios como los mercados en línea [...] que dan a consumidores [...] y empresas la capacidad de comunicar entre sí y con otros servicios de alojamiento de datos, incluso en los casos en que el servicio se presta a través de la computación en la nube, así como las plataformas de juegos y de juegos de apuestas en línea. No deben entrar en el ámbito de la definición, aunque entren en el ámbito de la definición de servicios de la sociedad de la información con arreglo a la Directiva (UE) 2015/1535, los casos en que el proveedor de servicios de la sociedad de la información no dé a sus usuarios la capacidad de comunicar entre sí sino únicamente con el proveedor del servicio, o no les dé la capacidad de tratar o almacenar datos, o el caso en que la capacidad de almacenar o tratar datos no sea una parte esencial del servicio que se presta a los usuarios, como los servicios jurídicos, de arquitectura, de ingeniería y de contabilidad prestados en línea y a distancia. [...]**
- (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 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.
- (24 bis) En la medida en que los procedimientos relativos a una solicitud de asistencia judicial pueden considerarse procedimientos en materia penal conforme a la legislación nacional de los Estados miembros, debe aclararse que no debe emitirse una orden europea de entrega ni de conservación con la finalidad de facilitar asistencia judicial a otro Estado miembro o tercer país. En dichos casos la solicitud de asistencia judicial debe dirigirse al Estado miembro o tercer país que pueda prestar asistencia judicial con arreglo a su legislación nacional. No obstante, si la autoridad emisora ya ha obtenido pruebas electrónicas en virtud del presente Reglamento para sus propias investigaciones o procesos penales y posteriormente dichas pruebas son objeto de transferencia o transmisión, deben aplicarse los requisitos del principio de especialidad.**
- (24 ter) El presente Reglamento debe aplicarse a los procedimientos penales iniciados por la autoridad emisora con objeto de localizar a un delincuente que haya sido condenado y haya huido de la justicia a fin de ejecutar una pena o una medida de seguridad privativa de libertad. Sin embargo, en caso de que la pena o la medida de seguridad se dictara en ausencia no debe ser posible emitir una orden europea de entrega ni de conservación habida cuenta de que la legislación nacional de los Estados miembros sobre las sentencias dictadas en ausencia varían considerablemente entre unos países y otros en toda la Unión Europea.**
- (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 [...] basarse [...] **en criterios objetivos específicos como** 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 mercantil¹⁴. Por otra parte, la prestación del servicio con vistas a la mera observancia de la prohibición de discriminación establecida en el Reglamento (UE) 2018/302¹⁵ 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, **teniendo debidamente en cuenta el impacto de la medida en los derechos fundamentales de la persona cuyos datos se solicitan.**

¹⁴ [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).

¹⁵ [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.º 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (DO L 601 de 2.3.2018, p. 1).

- (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 comunicación 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.
- (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.
- (33 bis) En los casos en que se emita una orden para obtener diferentes categorías de datos, la autoridad emisora debe garantizar que las condiciones y procedimientos, como la notificación al Estado de ejecución, se cumplen para cada una de las categorías de datos.**

- (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.
- (34 bis) En caso de que los datos se almacenen o traten como parte de una infraestructura facilitada por un proveedor de servicios a una autoridad pública, únicamente podrán emitir una orden europea de entrega o de conservación las autoridades de ese Estado miembro ya que los datos citados pueden considerarse especialmente sensibles. Debe entenderse por autoridad pública toda autoridad que, en virtud de su legislación nacional, tenga la facultad de regular o administrar una parte o un aspecto de la vida pública, como las ramas de los poderes judicial, legislativo o ejecutivo de un Estado, provincia o municipio.**
- (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 **o el derecho de los periodistas a no revelar sus fuentes de información**) 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. [...] **La necesidad de tener en cuenta un segundo marco jurídico debe depender de la fuerza de la vinculación de la persona cuyos datos se solicitan al Estado emisor. Cuando la persona reside en el territorio del Estado emisor, existe un fuerte vínculo con el Estado emisor. El marco jurídico aplicable a la evaluación de los privilegios e inmunidades debe ser por tanto únicamente el del Estado emisor. El mismo principio se aplica a las normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, y los intereses fundamentales del Estado de ejecución. En el momento en que se envíe una solicitud de datos de contenido o de transacciones, las autoridades ya dispondrán en general de una indicación de dónde reside la persona basada en las investigaciones previas. Además, las estadísticas muestran que en una gran mayoría de los casos, la persona reside en el Estado emisor. Cuando no es el caso, por ejemplo porque la persona cuyos datos se solicitan ha iniciado acciones para ocultar su ubicación, debe aplicarse el mismo principio.**

(35 bis) Los privilegios e inmunidades, así como las normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, que protegen [...] los datos de transacciones o los datos de contenido en el Estado [...] de ejecución, deben **por tanto** tenerse en cuenta [...] **cuando la autoridad emisora tenga motivos razonables para creer que la persona cuyos datos se solicitan no reside en su territorio.** [...] Esto es relevante, en particular, en caso de que la legislación de **aquel**[...] Estado miembro [...] ofrezca una mayor protección que la legislación del Estado emisor. La disposición también contempla los casos en que la comunicación de los datos pueda afectar a intereses fundamentales de dicho Estado miembro, como la seguridad y defensa nacionales. [...] **La autoridad de ejecución deberá tener en cuenta estos aspectos, no solo en el momento de emitirse la orden, sino también posteriormente, [...] y en caso de que se haya iniciado un procedimiento de ejecución.**

(35 ter) Cuando la autoridad emisora trate de obtener datos de transacciones y tenga motivos razonables para creer que la persona cuyos datos se solicitan no reside en su territorio y que los datos solicitados están protegidos por privilegios e inmunidades otorgados en virtud de la legislación del Estado de ejecución, o por las normas de dicho Estado miembro sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, o su comunicación pueda afectar a intereses fundamentales de dicho Estado miembro, como la seguridad y la defensa nacionales, la autoridad emisora debe solicitar aclaraciones, en particular mediante consultas oportunas.

(35 quater) En los casos en que la orden europea de entrega afecte a datos de contenido y en que la autoridad emisora tenga motivos razonables para creer que la persona cuyos datos se solicitan no reside en su territorio, ello se notificará al Estado de ejecución quien podrá, lo antes posible y preferentemente en un plazo de diez días, informar a la autoridad emisora de los elementos que podrían motivar la retirada o la adaptación de la orden, como pueden ser los privilegios e inmunidades de la persona cuyos datos se solicitan o las normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios. Al contrario que los datos sin contenido, los datos de contenido son de carácter especialmente sensible ya que las personas pueden revelar en ellos lo que piensan, así como detalles sensibles de su vida privada, Lo que justifica un tratamiento diferente y una implicación de las autoridades del Estado de ejecución en el procedimiento desde una fase temprana. En estos casos, el Estado miembro emisor debe facilitar una copia del certificado al Estado de ejecución en el momento en que entrega el certificado al proveedor de servicios. Si es necesaria una traducción del certificado, con objeto de facilitar una rápida comprobación, la autoridad emisora debe elegir una de las lenguas aceptadas por el Estado de ejecución, aun cuando el proveedor de servicios indicara que también aceptaría certificados en una lengua diferente de las lenguas oficiales del Estado de ejecución. Cuando la autoridad notificada presente los elementos citados, deberá facilitar a la autoridad emisora toda la información pertinente acerca de los privilegios e inmunidades, así como las normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, otorgados a la persona en virtud de su legislación en materia de información, o bien si la orden puede afectar a intereses fundamentales de dicho Estado miembro, como la seguridad y la defensa nacionales.

(35 quinquies) Los procedimientos descritos anteriormente no serán aplicables en los casos en que la persona, en el momento de emisión de la orden europea de entrega, tenga más de una residencia, una de las cuales esté situada en el territorio del Estado emisor, o en los casos en que la residencia de la persona no pueda determinarse con esfuerzos razonables y proporcionados. No obstante, una visita breve, unas vacaciones o una estancia similar en el Estado emisor sin la existencia de otros vínculos sustanciales no bastan para establecer la residencia en dicho Estado miembro.

(35 sexies) Con objeto de facilitar un procedimiento rápido, el momento pertinente para determinar si es necesario proceder a la notificación de las autoridades del Estado de ejecución debe ser el momento en el que se emite o se valida la orden. Cualquier cambio de residencia posterior no debe afectar al procedimiento. Cuando la autoridad emisora no dispusiera de motivos razonables para creer que la persona cuyos datos se solicitan no residía en su territorio en el momento de emisión o validación de la orden, y se sepa posteriormente que dicha persona de hecho no residía en el territorio del Estado miembro emisor, no debe requerirse ninguna otra comprobación o notificación posterior. No obstante, la persona afectada puede invocar sus derechos, así como las normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, durante todo el procedimiento penal, del mismo modo que el otro Estado miembro puede invocar sus intereses fundamentales, como la seguridad y la defensa nacionales, en cualquier momento del procedimiento penal. Además, estos motivos pueden invocarse asimismo durante el procedimiento de ejecución.

(35 septies) Cuando los datos estén protegidos por privilegios e inmunidades, o por normas sobre la determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios, otorgados por la legislación del Estado de ejecución, o bien cuando la comunicación de los datos pueda afectar a intereses fundamentales de dicho Estado miembro, el Estado emisor debe garantizar que estos motivos se tienen en cuenta del mismo modo que si estuvieran contemplados en su propia legislación nacional, al objeto de darles efecto. Si, por ejemplo, la legislación del Estado miembro emisor no otorga dichos privilegios e inmunidades, la protección debe, en la medida de lo posible, adaptarse al privilegio o inmunidad más cercano de acuerdo con la legislación del Estado emisor, teniendo en cuenta las finalidades e intereses que se persiguen mediante la protección específica y los efectos que de ella se derivan. En estas situaciones similares, deben aplicarse las consecuencias jurídicas de su propia legislación nacional. A los efectos de determinar el modo de tener en cuenta estos motivos al igual que si los contemplara su legislación nacional, la autoridad emisora podrá ponerse en contacto con la autoridad notificada y solicitar información adicional sobre el carácter y los efectos de la protección, ya sea directamente o por medio de la Red Judicial Europea o de Eurojust. Si bien el Estado emisor puede presentar cualquier o cualesquiera objeciones basadas en estos motivos, la persona cuyos datos se solicitan puede invocar únicamente sus derechos, como los privilegios e inmunidades, y no puede presentar objeciones basadas en un interés fundamental del Estado de ejecución.

(35 octies) Cuando un privilegio o inmunidad prohíba el uso de los datos, pero ese derecho pueda suspenderse, y cuando la autoridad emisora tenga intención de utilizar los datos obtenidos como prueba o no retire la orden en caso de no haber obtenido los datos, el Estado miembro emisor debe tener aún la posibilidad de solicitar a la autoridad competente que se suspenda el privilegio o la inmunidad.

(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.

(36 bis) Con objeto de garantizar la plena protección de los derechos fundamentales, la validación de una orden europea de entrega o de conservación por parte de una autoridad judicial debe obtenerse en principio antes de que se emita la orden. Podrán existir excepciones a este principio únicamente en casos excepcionales en los que se soliciten datos de abonado y datos de acceso, la autoridad emisora establezca válidamente que se trata de un caso urgente y no exista la posibilidad de obtener a tiempo una validación previa de la autoridad judicial, en particular porque no se pueda comunicar con la autoridad de validación para obtenerla y que la amenaza sea tan inminente que requiera acción inmediata. No obstante, esta disposición se aplica únicamente cuando el procedimiento está contemplado en un caso similar en la legislación nacional.

- (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. **Cuando una orden europea de entrega o de conservación se remita al proveedor de servicios a raíz del incumplimiento por parte del representante legal, también podrá aplicarse respecto a dicho proveedor de servicios.**
- (38) Las órdenes europeas de entrega y las órdenes europeas de conservación deberán transmitirse al [...] **destinatario** a través de un certificado de orden europea de entrega (EPOC) o un certificado de orden europea de conservación (EPOC-PR), que deberán traducirse. El certificado contendrá 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, con el fin de no poner en riesgo las investigaciones. Pero como forman parte de la propia orden, permiten al sospechoso impugnarla ulteriormente durante el proceso penal. En caso necesario, los certificados deberán traducirse a la lengua oficial del [...] **Estado de ejecución**, o a una de ellas, o a otra lengua oficial que el proveedor del servicio haya declarado aceptar.
- (39) La autoridad emisora competente **o la autoridad competente para la transmisión** deberá transmitir el EPOC o el EPOC-PR directamente al destinatario **de forma segura y fiable** 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 **de una forma segura y fiable que permita establecer la autenticidad del remitente y la integridad de los datos** 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 de la [...] **orden europea de entrega** 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.
- (41bis) El destinatario no deberá estar obligado a cumplir con una orden cuando haya una imposibilidad de hecho que no haya sido originada por el destinatario o por el proveedor de servicios, en caso de ser diferentes, en el momento en que se recibió la orden. Deberá asumirse la existencia de una imposibilidad de hecho en caso de que la persona cuyos datos fueron solicitados no sea cliente del proveedor de servicios o no fuese posible identificar a dicha persona como cliente incluso después de haberse solicitado informaciones complementarias a la autoridad emisora, o si los datos se han suprimido legalmente antes de recibirse la orden.**
- (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. **Además, deberán** [...] 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) 2016/679¹⁶. [...] **excepto cuando la autoridad emisora solicite que se informe a la persona.** En tales casos, la autoridad emisora proporcionará al proveedor de servicios la información necesaria sobre las vías de recurso a su disposición con el fin de que puedan incluirse en la información transmitida a dicha persona. **Encualquier caso**, 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 **no** se pidió[...] al proveedor de servicios que no informe al usuario, [...] **en cuanto** 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) 2016/680¹⁷. **La autoridad emisora podrá abstenerse de informar a aquellas personas cuyos datos relativos a los abonados y datos relativos al acceso fueran solicitados cuando se considere necesario y proporcionado para proteger los derechos fundamentales e intereses legítimos de otra persona y, en particular si tales derechos e intereses priman sobre el interés de ser informada de la persona cuyos datos se solicitan.** Tal podría ser el caso cuando una orden afecte a los datos relativos a los abonados o a los datos relativos al acceso de un tercero, teniéndose en cuenta la presunción de inocencia del sospechoso. Cuando la autoridad emisora desconozca la identidad de la persona de que se trate, solo podrán emprenderse investigaciones para determinarla cuando se considere necesario y proporcionado en relación con el carácter invasivo de la medida y con el correspondiente esfuerzo asociado al establecimiento de su identidad.
- (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.

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 (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1.

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, DO L 119 de 4.5.2016, p. 89.

- (45) El procedimiento de ejecución es un procedimiento por el que el destinatario puede[...] **invocar motivos formales contra** la ejecución en virtud de determinados motivos restringidos. La autoridad de ejecución podrá negarse a reconocer y ejecutar la orden por los mismos motivos, [...] **y también cuando deban ser tenidos en cuenta en virtud del presente Reglamento**, si se aplican privilegios e inmunidades **o normas en materia de determinación y limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios de comunicación** 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 ser proporcionadas, también a la vista de circunstancias específicas tales como el incumplimiento repetido o sistemático.
- (45bis) Al determinar en cada caso la sanción pecuniaria, las autoridades competentes deberán tener en cuenta todas las circunstancias pertinentes, como por ejemplo la naturaleza, la gravedad y la duración de la infracción, si se ha cometido intencionadamente o por negligencia, si el prestador de servicios ha sido considerado responsable de las infracciones anteriores similares y la solidez financiera del proveedor del servicio responsable. En circunstancias excepcionales, dicha valoración puede llevar a la autoridad de ejecución a optar por abstenerse de imponer sanciones pecuniarias. Deberá prestarse una especial atención, a este respecto, a las microempresas y a las empresas que incumplan una orden en situación de emergencia debido a la falta de recursos personales fuera del horario normal de oficina, si los datos se transmiten sin demora injustificada.**
- (46) Los proveedores de servicios no deberán considerarse responsables en los Estados miembros por el perjuicio causado a sus usuarios o a terceras partes derivado [...] del cumplimiento de buena fe de un EPOC o un EPOC-PR. **La responsabilidad de garantizar la legalidad de la orden, en particular su necesidad y proporcionalidad, recaerá en la autoridad emisora.**
- (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 [...] **podrá** 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 **de la legislación del país tercero son de aplicación, y, en caso afirmativo, si** 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.
- [...] [...] 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. **Especial importancia deberá concederse a la protección de los derechos fundamentales en las disposiciones y otros intereses esenciales del tercer país, como por ejemplo sus intereses en materia de seguridad nacional, así como el grado de vinculación de la causa penal a cualquiera de las dos jurisdicciones cuando se realice la evaluación.**

- (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 p[...]odría ejercerse [...] **cuando los datos obtenidos se utilicen en procesos penales contra ellos**. 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 **cuyos datos se soliciten pero** 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) [...] Durante el procedimiento de ejecución **la autoridad de ejecución podrá denegar el reconocimiento y ejecución de una orden europea de entrega o de conservación por una serie limitada de motivos** [...]
- (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.

- (56bis)** La transmisión, transferencia y utilización de pruebas electrónicas obtenidas a través de una orden europea de entrega en otros procedimientos o para otros fines distintos de aquellos para los que la orden fue emitida deberá limitarse, en particular, a las infracciones penales respecto de las que la autoridad emisora podría haber emitido una orden europea de una orden europea de entrega. La utilización, transmisión o transferencia de pruebas electrónicas deberá, además, ser únicamente posible en aquellos casos necesarios para evitar una amenaza grave para la seguridad pública de los respectivos Estados miembros o del tercer país, así como para sus intereses fundamentales. La transferencia internacional de pruebas electrónicas está además sujeta a las condiciones que figuran en el capítulo V de la Directiva (UE) 2016/680. En aquellos casos en que los datos personales obtenidos se utilicen para la prevención de una amenaza grave e inmediata para la seguridad pública de los respectivos Estados miembros o del tercer país y dicha amenaza no permita entablar investigaciones penales, será de aplicación el Reglamento (UE) 2016/679.
- (56ter)** Al realizar una declaración sobre el régimen lingüístico, se alienta a los Estados miembros a que incluyan al menos una lengua adicional a su lengua o lenguas oficiales.
- (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 legislación¹⁸. 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 Consejo¹⁹ para obtener pruebas electrónicas. Las autoridades de los Estados miembros deberán elegir el instrumento más adaptado al [...] **asunto de que se trate**; 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.

¹⁸ DO L 123 de 12.5.2006, p. 1.

¹⁹ [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.

- (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, [...] Irlanda ha 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, y el Reino Unido [...] no participará en la adopción del presente Reglamento y no queda vinculado por este ni sujeto 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.º 45/2001 del Parlamento Europeo y del Consejo²⁰, emitió un dictamen el (...) ²¹,

²⁰ 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.

²¹ 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 inculcadas 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.
- 2) «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.
- 3) «Proveedor de servicios»: persona física o jurídica que presta uno o más de los tipos de servicios siguientes, **a excepción de los servicios financieros a que se refiere el artículo 2, apartado 2, letra b), de la Directiva 2006/123/CE**:
 - 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 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;**
- c) **otros** 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 Consejo²², **que:**
 - **ofrecen a sus usuarios la capacidad para comunicarse entre ellos;**
o
 - la capacidad para procesar o almacenar datos por cuenta de los usuarios a los que se presta el servicio [...]²³.
- 4) «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 **basada en criterios objetivos específicos** con los Estados miembros a que se refiere la letra a).
- 5) «Establecimiento» o «**estar establecido**»: 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 [...] se gestiona la actividad.
- 6) «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.

²² [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).

²³ Finlandia, Letonia y Luxemburgo mantienen una reserva porque no debería obligarse a las autoridades públicas a cumplir una orden europea de entrega o de conservación (Finlandia), porque la definición sigue siendo muy vaga e incierta desde el punto de vista jurídico (Luxemburgo) y por la necesidad de analizar la definición más a fondo, especialmente en lo que respecta 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 (Letonia).

- 7) «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 autenticación utilizados en lugar de una contraseña que hayan sido facilitados por el usuario o creados a petición del usuario.
- 8) «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. Se incluyen aquí los metadatos de las comunicaciones electrónicas, según se definen en el artículo 4, apartado 3, letra [...]c), 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 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 [...]c), del [Reglamento relativo al respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas].
- 10) «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.
- 11) «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 Consejo²⁴.
- 12) «Estado emisor»: Estado miembro en el que se emita una orden europea de entrega o una orden europea de conservación.

²⁴ [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).

- 13) «Estado de ejecución»: Estado miembro en el que resida o esté establecido el destinatario de una orden europea de entrega o de una orden europea de conservación o al que, **de ser necesario**, 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.
- 14) «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.
- 15) «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 Consejo²⁵.

Artículo 3 *Ámbito de aplicación*

1. El presente Reglamento se aplicará a los proveedores que ofrezcan servicios en la Unión.
- 1 bis. El Reglamento no se aplicará a los procesos iniciados por la autoridad emisora con el fin de prestar asistencia judicial mutua a otro Estado miembro o a un país tercero.**
2. Una orden europea de entrega o una orden europea de conservación solo podrá emitirse para procesos penales [...] **y para la ejecución de penas de privación de libertad o de medidas de seguridad privativas de libertad que no se dictaron en rebeldía en caso de que la persona condenada hubiera huido de la justicia.** [...] 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 emisor²⁶.
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.

²⁵ [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).

²⁶ Chequia, Finlandia, Letonia y Alemania mantienen una reserva sobre la ampliación del ámbito de aplicación en relación con las personas condenadas que huyeron de la justicia, que también se aplica a las disposiciones paralelas del artículo 5, apartado 3, y del artículo 6, apartado 2.

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), al apartado 2, letra b), y al 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.
5. **En casos urgentes debidamente establecidos, las autoridades mencionadas en virtud del apartado 1, letra b, y del apartado 3, letra b) podrán emitir la orden respectiva para datos de los abonados y datos relativos al acceso, sin validación previa cuando la validación no pueda obtenerse a tiempo y cuando dichas autoridades puedan emitir la orden en un caso interno similar sin validación. La autoridad emisora solicitará la validación posterior sin demora indebida, a más tardar en un plazo de 48 horas. Cuando no se conceda dicha validación posterior, la autoridad emisora retirará la orden de forma inmediata y, de conformidad con su Derecho interno, suprimirá los datos obtenidos o garantizará que esos datos no se utilicen como prueba²⁷.**
6. Cada Estado miembro podrá designar a una o más autoridades centrales encargadas de la transmisión administrativa de certificados, órdenes y notificaciones, de la recepción de datos y notificaciones y de la transmisión de otra correspondencia oficial relativa a los certificados o las órdenes.

²⁷ Grecia y Luxemburgo mantienen una reserva sobre la posibilidad de solicitar la validación posterior.

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 **y para la ejecución de una pena de privación de libertad o de una medida de seguridad privativa de libertad de al menos cuatro meses.**
4. Solo podrá emitirse una orden europea de entrega con respecto a datos de transacciones o datos relativos al acceso para²⁸:
 - a) infracciones penales punibles en el Estado emisor con una pena máxima de privación de libertad de al menos tres años²⁹; 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 Consejo³⁰;
 - las definidas en los artículos 3 a 7 de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo³¹;
 - las definidas en los artículos 3 a 8 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo;

²⁸ Finlandia y Eslovenia preferirían que se creara una lista.

²⁹ Chipre mantiene una reserva relativa a las condiciones para emitir una orden europea de entrega para las infracciones penales punibles con una pena inferior a cinco años.

³⁰ [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).

³¹ [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).

- c) las infracciones penales definidas en los artículos 3 a 12 y 14 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo³²;
 - d) **la ejecución de una pena de privación de libertad o de una medida de seguridad privativa de libertad de al menos cuatro meses impuesta por infracciones penales en virtud de las letras a), b) y c) del presente apartado.**
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) **el usuario, excepto cuando la única finalidad de la orden sea identificar al usuario, o cualquier otro identificador único como el nombre de usuario, el identificador o el nombre de la cuenta a fin de determinar los datos solicitados [...];**
 - 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;
 - 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.

³² [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).

- 6 bis.** Una orden europea de entrega de datos almacenados o tratados en el marco de una infraestructura prestada por un proveedor de servicios a una autoridad pública solo podrá emitirse si la autoridad pública para la que se almacenan o procesan los datos se encuentra en el Estado emisor.
- 7.** [...] Cuando la orden se refiera a datos de transacciones y cuando la autoridad emisora se base en [...] motivos fundados para creer que [...] la persona de la que se solicitan los datos no reside en el territorio del Estado miembro emisor, y
- a. los datos solicitados estén protegidos por privilegios e inmunidades concedidos en virtud de la legislación del Estado [...] de ejecución o estén sujetos, en dicho Estado miembro, a normas sobre la determinación y la limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios de comunicación, o cuando su revelación pueda afectar a intereses fundamentales del [...] Estado de ejecución como la seguridad y la defensa nacionales, la autoridad emisora [...] pedirá aclaraciones sobre las circunstancias a que hace referencia el presente punto antes de emitir la orden europea de entrega, incluso mediante consulta a las autoridades del Estado [...] de ejecución [...], bien directamente o bien a través de Eurojust o de la Red Judicial Europea. Si la autoridad emisora considera que los datos [...] de transacciones [...] solicitados están protegidos por tales privilegios e inmunidades o por normas sobre la determinación y la limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios de comunicación, o que su revelación afectaría a los intereses fundamentales del otro Estado miembro como la seguridad y la defensa nacionales, tendrá en cuenta estas circunstancias del mismo modo que si se contemplaran en su Derecho interno y no emitirá o adaptará la orden europea de entrega cuando sea necesario para dar efecto a estos motivos³³.
- 8.** Cuando la retirada del privilegio o de la inmunidad competa a una autoridad del Estado de ejecución, la autoridad emisora podrá solicitar a la autoridad de ejecución que se ponga en contacto con la autoridad competente para pedirle que ejerza su competencia sin demora. Cuando la retirada del privilegio o de la inmunidad competa a una autoridad de otro Estado miembro, a un país tercero o a una organización internacional, la autoridad emisora podrá solicitar a la autoridad de que se trate que ejerza dicha competencia.

³³ Alemania y Chequia propusieron la inclusión de datos de contenido. Alemania también solicitó que se incluya una cláusula sobre los derechos fundamentales, tanto en esta disposición como en el artículo 12 *bis*. Hungría introdujo una reserva de fondo dada la lógica de la disposición, puesto que, a su entender, cuando existen motivos fundados para creer que la denegación es previsible, debería ser posible realizar una consulta previa en sentido general, también para las disposiciones paralelas en el artículo 5, apartado 7, el artículo 7 *bis*, el artículo 9, apartado 5 y los artículos 12 *bis* y 14.

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. **El artículo 5, apartado 6 bis, se aplicará *mutatis mutandis*.**
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, **así como para la ejecución de una pena de privación de libertad o una medida de seguridad privativa de libertad de duración no inferior a cuatro meses.**
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) [...] **el usuario**, excepto cuando la única finalidad de la orden sea identificar [...] **al usuario, o cualquier otro identificador único, como el nombre de usuario, el identificador de usuario o el nombre de la cuenta, a fin de determinar los datos solicitados;**
 - 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 [...], 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 ejecute un EPOC en un caso urgente con arreglo al artículo 9, apartado 2, la orden **europea de entrega** 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 7 bis
*Notificaciones*³⁴

1. **En los casos en que la orden europea de conservación se refiera a datos de contenido y la autoridad emisora tenga motivos razonables para creer que la persona cuyos datos se solicitan no reside en su territorio, la autoridad emisora remitirá una copia del EPOC a la autoridad competente del Estado de ejecución de forma simultánea al envío del EPOC al destinatario con arreglo al artículo 7.**
2. **La autoridad notificada podrá informar lo antes posible a la autoridad emisora de cualquier circunstancia prevista en el artículo 5, apartado 7, letra b) y procurará hacerlo en un plazo máximo de diez días. La autoridad emisora tendrá en cuenta las circunstancias notificadas del mismo modo que si estuvieran previstas en su Derecho interno y, si aún no se han facilitado los datos, retirará la orden o la adaptará, si procede, para dar efecto a estos motivos. En caso de retirada de la orden, la autoridad emisora lo notificará de inmediato al destinatario.**
3. **Cuando la retirada del privilegio o de la inmunidad compete a una autoridad del Estado de ejecución, la autoridad emisora podrá solicitar a la autoridad notificada que se ponga en contacto con la autoridad competente para pedirle que ejerza su competencia sin demora. Cuando la retirada del privilegio o de la inmunidad compete a una autoridad de otro Estado miembro, a un país tercero o a una organización internacional, la autoridad emisora podrá solicitar a la autoridad de que se trate que ejerza dicha competencia.**
4. **La notificación no tendrá efecto suspensivo en lo que respecta a las obligaciones del destinatario en virtud del presente Reglamento.**

³⁴ La República Checa, Finlandia, Alemania, Grecia, Hungría y Letonia han formulado una reserva sobre el procedimiento de notificación y abogan por un procedimiento con más efectos que incluya también los datos de transacciones y una cláusula en materia de derechos fundamentales que prevea una serie de motivos de denegación a los que pueda recurrir la autoridad notificada; también abogan por eliminar la norma sobre lo que debe considerarse un «caso nacional»; por último, Alemania es partidaria de que se presente la orden en lugar del certificado, mientras que la República Checa considera que se deben presentar tanto la orden como el certificado. Bélgica, Bulgaria, Estonia, Francia, Irlanda, Italia, Polonia, Portugal y España han formulado una reserva en relación con el procedimiento de notificación y las disposiciones relativas a la introducción de un procedimiento de notificación, en particular el artículo 5, apartado 7, y los artículos 9, 12 *bis* y 14, así como los considerandos correspondientes, y consideran preferible la propuesta de la Comisión, que no preveía la notificación. Bélgica, Luxemburgo, Irlanda, Eslovenia y Polonia consideran que, de mantenerse la notificación, esta debe dirigirse al Estado miembro en que resida la persona cuyos datos se solicitan.

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 o el EPOC-PR serán transmitidos por **la autoridad emisora o en su nombre [...]** por cualquier medio **seguro y fiable que permita [...]** al destinatario **dejar constancia escrita** y determinar [...] la autenticidad **del certificado**.

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 **por un medio seguro y fiable que permita determinar la autenticidad y la integridad**, 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 rápida³⁵.
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 [...] una imposibilidad material **que se derive de circunstancias no creadas por el destinatario o por el proveedor de servicios en el momento de recepción de la orden** [...], el destinatario informará a la autoridad emisora citada en el EPOC sin demora indebida y explicando las razones, mediante el formulario que figura en el anexo III. [...]

³⁵ Alemania propone añadir al menos un nuevo considerando en el que se pida a la Comisión y a los Estados miembros que trabajen para establecer, lo antes posible, canales de comunicación electrónicos seguros que permitan determinar la autenticidad y la integridad.

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.

[...] ³⁶

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.

³⁶ Hungría ha formulado una reserva sobre esta supresión.

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 [...] una imposibilidad material **que se derive de circunstancias no creadas por el destinatario o por el proveedor de servicios en el momento de recepción de la orden** [...], el destinatario informará a la autoridad emisora citada en el EPOC sin demora indebida y explicando las razones, mediante el formulario que figura en el anexo III. [...]
6. En todos los casos en que, por otros motivos [...], 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*³⁷

1. El destinatario o, 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 [...] se abstendrá de informar a la persona cuyos datos se solicitan a fin de **evitar** [...] obstruir el proceso penal pertinente. **Únicamente informará a la persona cuyos datos se solicitan si así se lo pide expresamente la autoridad emisora. En tal caso, la autoridad emisora también proporcionará al destinatario o, en su caso, al proveedor de servicios la información prevista en el apartado 4 del presente artículo.**
2. Cuando la autoridad emisora **no** solicite al [...] **proveedor de servicios que informe** [...] a la persona cuyos datos se solicitan [...] **con arreglo al apartado 1**, será la autoridad emisora la que informe [...] a dicha persona [...]. **La autoridad emisora podrá retrasar la notificación a la persona cuyos datos se solicitan siempre que constituya una medida necesaria y proporcionada** [...] para evitar obstruir un proceso penal [...].
3. **La autoridad emisora podrá abstenerse de informar a la persona cuyos datos de abonado o cuyos datos relativos al acceso se solicitan cuando resulte necesario y proporcionado para la protección de los derechos fundamentales y los intereses legítimos de otra persona, y en particular cuando tales derechos e intereses prevalezcan sobre el interés de información de la persona cuyos datos se solicitan.** [...]
4. **Se incluirá información sobre las vías de recurso disponibles con arreglo al artículo 17.**

³⁷ Finlandia y Alemania han formulado reservas en las que propugnan un mayor nivel de detalle (disposiciones en materia de idioma, asistencia jurídica gratuita, información detallada sobre las vías de recurso, etc.). Además, Alemania considera que debe informarse a las personas afectadas (y no solo a las personas cuyos datos se solicitan).

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. **Los Estados miembros notificarán sus normas en materia de reembolso a la Comisión, que se encargará de publicarlas.**

Artículo 12 *bis* [...]
[...] **Restricciones al uso de los datos obtenidos**

1. [...] **Si la persona cuyos datos se solicitan no reside en el territorio del Estado emisor y a través de la orden europea de entrega se han obtenido [...] datos de transacciones o [...] datos de contenido [...] y la autoridad emisora recibe información de que tales datos [...] están protegidos por privilegios o inmunidades concedidos en virtud de la legislación del Estado [...] de ejecución, o están sujetos, en el Estado de ejecución, a normas sobre la determinación y la limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios de comunicación, o si dicho Estado miembro alega que la revelación de tales datos afectaría a sus intereses fundamentales [...], como la seguridad y la defensa nacionales, [...] las autoridades competentes del Estado emisor garantizarán durante el proceso penal [...] que esos motivos sean tenidos en cuenta en las mismas condiciones que si estuvieran previstos en su legislación nacional [...]. [...] Las autoridades competentes podrán consultar a las autoridades del Estado miembro de que se trate, a la Red Judicial Europea en materia penal o a Eurojust.**

2. **Cuando la retirada del privilegio o de la inmunidad competa a una autoridad del Estado de ejecución, la autoridad competente del Estado emisor podrá solicitar a la autoridad notificada o de ejecución que se ponga en contacto con la autoridad competente del Estado de ejecución para pedirle que ejerza su competencia sin demora. Cuando la retirada del privilegio o de la inmunidad competa a una autoridad de otro Estado miembro, a un país tercero o a una organización internacional, la autoridad competente del Estado emisor podrá solicitar a la autoridad de que se trate que ejerza dicha competencia.**

Artículo 12 ter
Principio de especialidad

1. **Las pruebas electrónicas no se utilizarán en el marco de un procedimiento distinto de aquel para el que fueron obtenidas con arreglo al presente Reglamento, excepto:**
 - a) **cuando se trate de un procedimiento para el que se podría haber emitido una orden europea de entrega con arreglo al artículo 5, apartados 3 y 4; o**
 - b) **para evitar una amenaza grave e inmediata para la seguridad pública o los intereses fundamentales del Estado emisor.**

2. **Las pruebas electrónicas obtenidas con arreglo al presente Reglamento únicamente podrán transmitirse a otro Estado miembro:**
 - a) **a los efectos de un procedimiento para el que se podría haber emitido una orden europea de entrega con arreglo al artículo 5, apartados 3 y 4; o**
 - b) **para evitar una amenaza grave e inmediata para la seguridad pública o los intereses fundamentales de dicho Estado miembro.**

3. **Las pruebas electrónicas obtenidas de conformidad con el presente Reglamento solo se podrán transferir a un país tercero o a una organización internacional con arreglo a las condiciones previstas en el apartado 2, letras a) y b) del presente artículo y el capítulo V de la Directiva (UE) 2016/680.**

Capítulo 3: Sanciones y ejecución

Artículo 13 *Sanciones*³⁸

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, **apartado 1**, del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Los Estados miembros comunicarán a la Comisión el régimen establecido y las medidas adoptadas, sin demora, y le notificarán sin demora cualquier modificación posterior.

Los Estados miembros se asegurarán de que las sanciones pecuniarias previstas [...] sean eficaces, proporcionadas y disuasorias.

Los Estados miembros se asegurarán de que se puedan imponer sanciones pecuniarias de hasta el 2 % del total del volumen anual de negocios mundial del ejercicio precedente del proveedor de servicios.

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 [...] **aceptadas por** [...] ese Estado miembro, e informará al destinatario del traslado.
2. Una vez recibida la documentación, la autoridad de ejecución reconocerá sin más trámites **y tomará las medidas necesarias para ejecutar:**
 - a) la orden europea de entrega, **salvo que la autoridad de ejecución considere que es aplicable alguno de los motivos previstos en el apartado 4, o**
 - b) **la orden europea de conservación, [...] salvo que la autoridad de ejecución considere que es aplicable alguno de los motivos previstos en el apartado [...] 5 [...].**

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.

³⁸ Finlandia, Alemania y Letonia mantienen una reserva sobre la armonización de las sanciones.

- 2 bis. El artículo 5, apartado 8, se aplicará *mutatis mutandis*.**
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 el apartado [...] 4, **letras a) a e)**, o en el **apartado 5**, así como de las sanciones aplicables en caso de incumplimiento, y establecerá un plazo para dar cumplimiento o manifestar la oposición.
4. [...] **Solo se podrá denegar el reconocimiento o** 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 penal prevista en el artículo 5, apartado 4;
 - c) el destinatario no pudo ejecutar el EPOC por imposibilidad material [...] 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) [...] **es de aplicación uno de los motivos mencionados en el artículo 12 bis, apartado 1.**³⁹
5. [...] **Solo se podrá denegar el reconocimiento o** 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 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) [...]

³⁹ La República Checa, Finlandia, Hungría, Alemania y Letonia mantienen una reserva sobre la supresión del artículo 14, apartado 4, letra f), y apartado 5, letra e), alegando que solo podrían apoyar la supresión si se añadiera una cláusula sobre los derechos fundamentales y el respeto de las normas constitucionales nacionales en el artículo 5, el artículo 7 bis, apartado 2, y el artículo 12 bis, apartado 1.

6. En caso de oposición del destinatario, **de conformidad con el apartado 4, letras a) a e), y el apartado 5**, 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 **o por normas sobre la determinación y la limitación de la responsabilidad penal en relación con la libertad de prensa y la libertad de expresión en otros medios de comunicación** 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

[...]

[...]

[...]

Artículo 16

Procedimiento de reexamen en caso de obligaciones contradictorias [...]

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 [...], 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, apartados 5 y 6.
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. **Deberá presentarse a más tardar en un plazo de diez días a partir de la fecha en la que el destinatario recibió la notificación de la EPOC. Los plazos deberán calcularse de conformidad con el Derecho nacional de la autoridad emisora.**
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:
- a) es aplicable la legislación del país tercero, según las circunstancias específicas del caso de que se trate y, en caso afirmativo,
 - b) 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: **La evaluación se basará [...], en particular, en los siguientes elementos, aunque se dará mayor peso a los elementos mencionados en las letras a) y b):**
- a) el interés protegido por la legislación pertinente del país tercero, en particular **los derechos fundamentales y otros intereses que impiden [...] la revelación de los datos, especialmente los intereses de seguridad nacional del país tercero;**
 - 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.

- 5 bis.** El órgano jurisdiccional podrá solicitar información a la autoridad competente del país tercero teniendo en cuenta la Directiva 2016/680, en particular su capítulo V, y en la medida en que dicha transmisión no obstaculice el proceso penal pertinente.
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 efectivas⁴⁰

1. **Sin perjuicio de otras vías de recurso posibles según el Derecho nacional, cualquier** [...] persona [...]cuyos datos hayan sido **solicitados** [...] mediante una orden europea de entrega tendrán derecho a vías de recurso efectivas contra dicha orden. **Si dicha persona es sospechosa [...] o acusada, tendrá derecho a vías de recurso efectivas** durante el proceso penal [...] para el que [...] **se estuvieran utilizando los datos. Dichas vías de recurso se entenderán** sin perjuicio de las vías de recurso disponibles con arreglo a la Directiva (UE) 2016/680 y al Reglamento (UE) 2016/679.
2. [...]
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.

⁴⁰ Alemania mantiene una reserva y afirma que toda persona sobre la que exista una orden debe tener derecho a una vía de recurso y no únicamente la persona sobre la que se solicitaron los datos y que también debería haber vías de recurso posibles en los procedimientos penales contra las órdenes de conservación.

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

[...]

[...]

Capítulo 5: Disposiciones finales

Artículo 18 bis

Idioma

Cada Estado miembro deberá indicar si, en caso de ejecución, acepta que la transmisión del EPOC o EPOC-PR o de la orden europea de entrega y de la orden europea de conservación se hagan en otro idioma distinto de su lengua o lenguas oficiales y, en caso de que así sea, en cuál.

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 de seguimiento establecerá los medios por los que se recopilarán los datos y otras pruebas necesarias, y la periodicidad de dicha recopilación. En él se especificarán las medidas que deban adoptar la Comisión y los Estados miembros a la hora de 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, **en la medida de lo posible**:
 - 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, **validación posterior**);
 - 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;
- f) **el número de casos en los que no se concedió una validación posterior.**

3. Los proveedores de servicios podrán recopilar, mantener y publicar estadísticas; si recopilan dichos datos deben enviarlos a la Comisión a más tardar el 31 de mayo de cada año para el año civil anterior y podrán incluir, en la medida de lo posible:

- a) **el número de EPOC y EPOC-PR recibidos por tipo de datos solicitados, por Estado miembro 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 Estado miembro y por situación (desglose entre casos urgentes y no urgentes);**
- c) **para los EPOC ejecutados, la duración media del tiempo empleado en proporcionar los datos solicitados desde el momento de recepción de la orden europea de entrega hasta el momento en que se facilitaron, por tipo de datos solicitados, por Estado miembro y por situación (desglose entre casos urgentes y no urgentes).**

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 los 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 al día siguiente 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 los 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 de 13 de abril de 2016 sobre la mejora de la legislación⁴¹.
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 y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

⁴¹ DO L 123 de 12.5.2016, p. 13.

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[...], validar, **transmitir o recibir** órdenes europeas de entrega y órdenes europeas de conservación **o sus notificaciones**;
 - 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 el artículo [...] 16;
 - d) **idiomas aceptados para la transmisión del EPOC o del EPOC-PR o de la orden europea de entrega y de la orden europea de conservación, en caso de ejecución de conformidad con el artículo 18 bis.**
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 Consejo⁴².

Artículo 23
Relación con [...] otros instrumentos jurídicos, acuerdos y pactos

El presente Reglamento no afecta a otros instrumentos jurídicos, acuerdos y pactos de la UE e internacionales [...] relativos a la obtención de pruebas que también estén contempladas en el ámbito de aplicación del presente Reglamento.

⁴² 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.

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 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 a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable una vez transcurridos *[[...]* **veinticuatro** *meses desde la fecha 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 Estrasburgo, el

Por el Parlamento Europeo

Por el Consejo

El Presidente / La Presidenta

El Presidente / La Presidenta
