Dictamen 23/2018 relativo a las propuestas de la Comisión Europea sobre las órdenes europeas de conservación y entrega de pruebas electrónicas a efectos de enjuiciamiento penal (artículo 70, apartado 1, letra b)

Adoptado el 26 de septiembre de 2018

Índice

El Supervisor Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra b, del 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,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

Introducción

En abril de 2018, la Comisión presentó una propuesta de Reglamento sobre las órdenes europeas de conservación y entrega de pruebas electrónicas a efectos de enjuiciamiento penal y una propuesta de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales. Las dos propuestas, COM (2018) 225 final y COM (2018) 226 final, son complementarias. El objetivo global perseguido por la Comisión consiste en mejorar la cooperación entre las autoridades de los Estados miembros y los proveedores de servicios, incluidos los de terceros países, y proponer soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio.

Mientras que el proyecto de Reglamento dispone las normas y los procedimientos aplicables a la emisión, notificación y ejecución de las órdenes de conservación y entrega de pruebas electrónicas a los proveedores de servicios de comunicación electrónica, el proyecto de Directiva establece unas normas mínimas para la designación de un representante legal de los proveedores de servicios no establecidos en la UE.

En noviembre de 2017[1], antes de que la Comisión presentara un proyecto de propuesta, el Grupo de Trabajo del artículo 29 (GT29) recordó la necesidad de garantizar que cualquier propuesta legislativa cumpla plenamente el acervo de la UE vigente en materia de protección de datos en particular, así como la legislación y la jurisprudencia de la UE en general.

Concretamente, el GT29 advirtió contra las limitaciones a los derechos a la protección de datos y la intimidad con respecto a los datos tratados por los proveedores de la sociedad de la información y de las telecomunicaciones, especialmente cuando sean tratados ulteriormente por las autoridades policiales; recordó la necesidad de garantizar la coherencia de cualquier instrumento de la UE con el vigente Convenio de Budapest del Consejo de Europa sobre la ciberdelincuencia y con la Directiva de la UE sobre la orden europea de investigación (OEI), y recomendó aclarar las respectivas normas procesales que regulan el acceso a las pruebas electrónicas a nivel nacional y de la UE para garantizar que el nuevo instrumento no conceda a las autoridades nuevas competencias de las que carecerían en su Derecho interno. Además de estas observaciones generales, el GT29 comentó las opciones legislativas examinadas por la Comisión en aquel momento sobre las categorías de los datos consideradas y las correspondientes garantías para acceder a ellos; la posibilidad de enviar las órdenes europeas de entrega/mandamientos de ejecución a los proveedores de servicios para que faciliten datos ubicados fuera de la Unión, y las condiciones sustantivas y de procedimiento de las garantías necesarias para salvaguardar el acceso directo a los datos.

[1] Véase GT 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

Ante las propuestas concretas sobre las pruebas electrónicas ahora presentadas, el SEPD desea proporcionar un análisis más detallado de la propuesta de instrumentos jurídicos desde el punto de vista de la protección de datos.

1. Base jurídica de la propuesta de Reglamento (artículo 82 del TFUE)

La base jurídica propuesta para el proyecto de Reglamento sobre las pruebas electrónicas es el artículo 82, apartado 1, del TFUE, relativo a la cooperación judicial en materia penal, que dispone lo siguiente:

> «1. La cooperación judicial en materia penal en la Unión se basará en el principio de reconocimiento mutuo de las sentencias y resoluciones judiciales e incluye la aproximación de las disposiciones legales y reglamentarias de los Estados miembros en los ámbitos mencionados en el apartado 2 y en el artículo 83.
>
> El Parlamento Europeo y el Consejo adoptarán, con arreglo al procedimiento legislativo ordinario, medidas tendentes a:
>
> a) establecer normas y procedimientos para garantizar el reconocimiento en toda la Unión de las sentencias y resoluciones judiciales en todas sus formas;
>
> b) prevenir y resolver los conflictos de jurisdicción entre los Estados miembros;
>
> c) apoyar la formación de magistrados y del personal al servicio de la administración de justicia;
>
> d) facilitar la cooperación entre las autoridades judiciales o equivalentes de los Estados miembros en el marco del procedimiento penal y de la ejecución de resoluciones.»

Como subraya la Comisión en la evaluación de impacto que acompaña a las propuestas, el artículo 82, apartado 1, especifica que la cooperación judicial en materia penal se basará en el principio de reconocimiento mutuo. Esta base jurídica cubriría la posible legislación sobre la cooperación directa con los proveedores de servicios, en la que la autoridad del Estado miembro de emisión se dirigiría directamente a una entidad (el proveedor de servicios) en el Estado de ejecución e incluso le impondría obligaciones. De este modo se introduciría una nueva dimensión en el reconocimiento mutuo, que trascendería la cooperación judicial tradicional en la Unión, basada hasta la fecha en procedimientos en los que participan dos autoridades judiciales, una en el Estado de emisión y otra en el Estado de ejecución.» (el subrayado es mío)

Habida cuenta de la novedad que representa la utilización de esta base jurídica en el contexto de las solicitudes directas entre autoridades públicas y entidades privadas, el SEPD lamenta que la Comisión no aporte ningún otro análisis ni evaluación.

En efecto, como ya subrayó el Grupo de Trabajo en su declaración previa, el SEPD sigue expresando sus dudas sobre la pertinencia de esta base jurídica, respaldadas por el análisis del TJUE y su Abogado General en el Dictamen 1/15. Entre los progresos realizados en relación con la validez del artículo 82 como base jurídica para el proyecto de Acuerdo PNR entre la UE y Canadá, el Tribunal subrayó que la autoridad canadiense competente «no constituye una autoridad judicial ni una autoridad

equivalente»[2]. En el contexto de las propuestas sobre las pruebas electrónicas, uno de los principales objetivos perseguidos declarados por la Comisión parece ser evitar una cooperación judicial «excesivamente complicada». Por consiguiente, la propuesta se basa en el principio de que la cooperación debe tener lugar entre una autoridad y un proveedor de servicios, y no entre dos autoridades. El procedimiento previsto sitúa, ante todo, a las entidades privadas en la posición de parte receptora que responde a las solicitudes de las autoridades judiciales.

El SEPD toma nota de que el procedimiento de ejecución de las órdenes de conservación y entrega de pruebas electrónicas podría implicar la participación de una autoridad receptora cuando el proveedor de servicios receptor de la orden no cumpla sus obligaciones, lo que daría lugar a la necesidad de ejecutar la orden *a posteriori*. Sin embargo, como el objetivo principal del procedimiento establecido consiste precisamente en no implicar a una autoridad receptora, el SEPD duda que este procedimiento auxiliar justifique la utilización del artículo 82 como única base jurídica del instrumento.

Por tanto, el SEPD opina que, para que el artículo 82 pueda utilizarse como base jurídica, las principales etapas del procedimiento de cooperación deben tener lugar entre dos autoridades judiciales, y que debe utilizarse otra base jurídica para este tipo de cooperación.

2. Necesidad de pruebas electrónicas en comparación con los tratados de asistencia jurídica mutua (TAJM) y la orden europea de investigación (OEI)

El SEPD toma nota de que la Comisión se ha comprometido a examinar los obstáculos a las investigaciones penales, en particular en lo que se refiere al acceso a las pruebas electrónicas. En su exposición de motivos, la Comisión presenta el contexto de la propuesta y subraya el carácter volátil de las pruebas electrónicas y su dimensión internacional, así como la necesidad de adaptar el mecanismo de cooperación a la era digital. Las propuestas de Reglamento y Directiva sobre la transmisión y el acceso a las pruebas electrónicas no están destinadas a sustituir a los instrumentos anteriores de cooperación en materia penal, tales como el Convenio de Budapest, los tratados de asistencia judicial mutua (TAJM) y la orden europea de investigación (OEI). Según la Comisión, las propuestas sobre las pruebas electrónicas tienen como objetivo mejorar la cooperación judicial en materia penal entre las autoridades y los proveedores de servicios en la Unión Europea, así como con los terceros países, en particular los Estados Unidos de América.

Dado que estas nuevas herramientas adicionales se dedicarán específicamente al acceso y la transmisión de pruebas electrónicas, el SEPD evaluará el valor añadido de estos instrumentos respecta de la OEI y los TAJM.

a) Necesidad de pruebas electrónicas en comparación con las garantías ofrecidas por la OEI y los TAJM

El principal argumento esgrimido por la Comisión en favor de las propuestas sobre las pruebas electrónicas es que se acelera el proceso para asegurar y obtener pruebas electrónicas almacenadas o en poder de proveedores de servicios establecidos en otra jurisdicción.

[2] Véase el punto 103 del Dictamen 1/15 y el punto 108 de las conclusiones del Abogado General en este asunto.

El SEPD lamenta, no obstante, que la necesidad de disponer de un nuevo instrumento para organizar el acceso a las pruebas electrónicas no se demostrara en la evaluación de impacto. De hecho, las propuestas carecen de una demostración de que no podría haberse utilizado ningún otro medio menos invasivo para alcanzar el objetivo en materia de pruebas electrónicas, aunque podrían haberse contemplado soluciones alternativas. Por ejemplo, podría haberse examinado la posibilidad de modificar y mejorar la Directiva sobre la OEI, respondiendo también al requisito específico de la Directiva sobre la OEI de evaluar la necesidad de modificar el texto antes del 21 de mayo de 2019[3]. Otra opción podría haber sido prever la utilización de órdenes de conservación para congelar los datos hasta que se expida una petición formal sobre la base de un TAJM. Estas opciones habrían permitido mantener las salvaguardias previstas en estos instrumentos, garantizando al mismo tiempo que los datos personales no se suprimirán.

El SEPD toma nota de que los plazos establecidos en la Directiva sobre la OEI son más largos que los de la propuesta sobre las pruebas electrónicas. De hecho, la autoridad de ejecución tiene treinta días para adoptar su decisión sobre el reconocimiento de la solicitud[4] y, a continuación, debe ejecutar la orden en el plazo de noventa días[5]. El SEPD considera que conceder treinta días de reflexión a las autoridades de ejecución en la OEI es una salvaguardia fundamental que permite determinar si la solicitud de ejecución está fundada y respeta todas las condiciones para la emisión y transmisión de una OEI.[6]

Al SEPD le preocupa que el plazo de diez días fijado en las propuestas para ejecutar el certificado de orden europea de entrega de datos (EPOC, por sus siglas en inglés), sin período de reflexión, impide la correcta apreciación de si el EPOC cumple todos los criterios y se ha cumplimentado correctamente.

Por lo tanto, el SEPD recomienda dar más tiempo al receptor del EPOC para determinar si la orden debe ejecutarse o no.

El SEPD toma nota de que, en el caso de la orden europea de conservación de datos (EPOC-PR, por sus siglas en inglés), no hay ninguna garantía de que la conservación de los datos se limite a lo que es necesario para su entrega. En efecto, la duración de la conservación de los datos podrá exceder de sesenta días, puesto que no hay límite de tiempo para que la autoridad de emisión informe al destinatario, se abstenga de emitir o retire una orden de entrega de pruebas electrónicas. Por consiguiente, el SEPD recomienda que al menos se fije un plazo para que la autoridad de emisión se abstenga o retire la orden de entrega a fin de cumplir con el principio de minimización de los datos establecidos en el Reglamento general de protección de datos[7].

Por último, el SEPD observa que la Directiva establece el retorno de las pruebas desde el Estado de emisión a la autoridad de ejecución[8]. Sin embargo, la propuesta de Reglamento sobre las pruebas electrónicas no dice nada sobre tal posibilidad. No queda claro qué ocurre con las pruebas electrónicas desde su transmisión a la autoridad de emisión.

Por lo tanto, el SEPD recomienda que la propuesta de Reglamento proporcione más información sobre el uso de las pruebas electrónicas después de su transmisión a la autoridad de emisión a fin de

[3] Véase el artículo 37 de la Directiva sobre la OEI.
[4] Artículo 12, apartado 3, de la Directiva sobre la OEI.
[5] Artículo 12, apartado 4, de la Directiva sobre la OEI.
[6] Artículo 6 de la Directiva sobre la OEI.
[7] Artículo 5 , apartado 1, letra a), del Reglamento general de protección de datos.
[8] Artículo 12, apartados 3 y 4, de la Directiva sobre la OEI.

cumplir con el RGPD y con el principio de transparencia[9], así como con el principio de especificidad establecido por los TAJM.

b) El abandono del principio de doble tipificación

El SEPD admite que el reconocimiento mutuo depende de la aplicación de la doble tipificación, que es una forma de que los Estados miembros mantengan su soberanía. No obstante, la doble tipificación se considera cada vez más un obstáculo a la cooperación judicial. Los Estados miembros de la UE están más dispuestos a cooperar, incluso aunque las medidas de investigación se refieran a actos que no se consideren como delito en su Derecho nacional. El SEPD recuerda, no obstante, que el principio de doble tipificación tiene por objeto proporcionar una salvaguardia adicional para garantizar que un Estado no pueda contar con la asistencia de otro para aplicar una sanción penal que no existe en el Derecho de este último Estado. Ello impide, por ejemplo, que un Estado exija la ayuda de otro para encarcelar a alguien por sus opiniones políticas cuando dichas opiniones no están tipificadas como delito en el Estado requerido o para procesar a una persona por haber abortado si esta persona reside en un Estado donde el aborto no es ilegal. El principio de doble tipificación va acompañado a menudo de limitaciones o salvaguardias adicionales relativas a las sanciones cuando estas difieren demasiado entre el Estado requirente y el Estado requerido. El principal ejemplo es el compromiso de no aplicar la pena de muerte de determinados TAJM cuando no existe en el Derecho de una de las dos Partes.

El SEPD toma nota de que el principio de doble tipificación está excluido de la propuesta de Reglamento sobre las pruebas electrónicas. La consecuencia, sin embargo, no es solo la supresión de los trámites de reconocimiento mutuo, sino también la supresión de las salvaguardias vinculadas al propio principio de doble tipificación.

En efecto, el SEPD observa que no se hace ninguna referencia a la ley del país en el que el proveedor de servicios está establecido, y que las órdenes de conservación de datos, así como de entrega de datos de los abonados o relativos al acceso a los datos, podrán emitirse para todos las infracciones penales[10], con independencia de que existan infracciones penales similares establecidas en otros Estados miembros o no.

Entretanto, las órdenes de entrega solo podrán emitirse y ejecutarse cuando exista una medida similar para la misma infracción penal en una situación comparable a nivel nacional en el Estado de emisión[11]. Además, tal como explica la Comisión en la exposición de motivos de la propuesta de Reglamento, se establece la especificidad de los datos de transacciones y los datos de contenido, que se consideran más sensibles. En efecto, las órdenes relativas a datos de transacciones o datos de contenido se basan en un umbral de una pena máxima de privación de libertad de al menos tres años, a fin de garantizar el respeto de la proporcionalidad y los derechos de las personas afectadas[12]. Sin embargo, el SEPD insiste en que no ha habido aún una armonización en la UE de los delitos castigados con una pena máxima de privación de libertad de al menos tres años.

El SEPD se opone al abandono del principio de doble tipificación, que tiene por objeto garantizar que un Estado no pueda invocar la ayuda de otros Estados para que su Derecho penal nacional sea aplicado fuera de su territorio por otro Estado que no comparte el mismo enfoque, habida cuenta, en

[9] Artículo5 , apartado 1, letra c), del Reglamento general de protección de datos.
[10] Artículo 5 , apartado 3, y artículo 6, apartado 2, de la propuesta de Reglamento sobre las pruebas electrónicas.
[11] Artículo 5 , apartado 3, de la propuesta de Reglamento sobre las pruebas electrónicas.
[12] Artículo 5 , apartado 4, de la propuesta de Reglamento sobre las pruebas electrónicas.

particular, de la desaparición de otras importantes salvaguardas tradicionales en el ámbito del Derecho penal (véase más adelante el punto 3 sobre los criterios de ubicación y el punto 7 g) sobre los posibles conflictos con el ordenamiento jurídico de terceros países).

c) La consecuencia de dirigirse a las empresas directamente

El SEPD reconoce que las pruebas electrónicas están cada vez más disponibles en infraestructuras privadas y pueden estar situadas fuera del país de la investigación, al ser propiedad de los proveedores de servicios.

El SEPD toma nota de que, tras las resoluciones adoptadas en Bélgica en los asuntos *Yahoo!*[13] *y Skype*[14], y en el contexto de los atentados terroristas, es necesaria una cooperación más ágil y rápida entre las entidades públicas y privadas. En la evaluación de impacto, la Comisión se refiere a tres tipos de instrumentos procesales que implican tanto a las autoridades públicas como a los proveedores de servicios. Se trata de la cooperación judicial, la cooperación directa y el acceso directo. Si en el primero de ellos la responsabilidad de ejecutar la OEI no recae en el proveedor de servicios, sino en la autoridad de ejecución[15], el segundo - la cooperación directa - se basa en la cooperación del proveedor de servicios. El más intrusivo desde la perspectiva del proveedor de servicios es el acceso directo, puesto que las autoridades públicas pueden acceder a los datos sin la ayuda de un intermediario.

Por tanto, el SEPD teme que, cuando se dirijan directamente a ellos, los proveedores de servicios no garantizarán la protección de los datos personales como las autoridades públicas pueden y están obligadas a hacer, y hace hincapié en que esto también supone la inaplicabilidad de determinadas garantías procesales previstas en el contexto de la cooperación judicial para los ciudadanos, así como para las propias empresas[16]. Efectivamente, por ejemplo, un proveedor de servicios requerido tendría que presentarse ante el órgano jurisdiccional de otro Estado (miembro) para impugnar la orden, mientras que en el marco de la cooperación judicial tendría que tratar con sus propias autoridades. El SEPD recomienda la inclusión de fundamentos adicionales en la propuesta de Reglamento, que acrediten que los proveedores de servicios protegerán los derechos fundamentales individuales, como la protección de los datos personales y el respeto de la vida privada y familiar, así como la información de la autoridad de protección de datos competente, a fin de asegurarse de que es posible un control.

3. El nuevo fundamento de la competencia judicial y la pretendida desaparición de los criterios de ubicación

El SEPD toma nota de que la Comisión subraya que uno de los principales cambios introducidos por estas propuestas es la desaparición de los criterios de ubicación y la posibilidad de que las

[13] Hof van Cassatie de Bélgica, YAHOO!Inc., n.º P.13.2082.N, de 1 de diciembre de 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen de Bélgica, n.º ME20.F1.105151-12 de 27 de octubre de 2016. (Skype ha recurrido contra la resolución).
[15] Artículos 10 a 16.
[16] Véase también, desde una perspectiva internacional de protección de datos, el «Documento de trabajo sobre normas para la protección de datos y la intimidad en las solicitudes de datos transfronterizas a efectos de enjuiciamiento penal», Grupo de Trabajo Internacional sobre protección de datos en las telecomunicaciones, 63ª reunión, 9-10 de abril de 2018, Budapest (Hungría).

autoridades competentes soliciten la conservación y la entrega de datos, con independencia de que dichos datos estén efectivamente almacenados.

Desde la perspectiva de la protección de datos, no constituye una novedad que la normativa europea de protección de datos se aplique con independencia de que los datos de las personas en cuestión estén almacenados. En efecto, la aplicabilidad del Reglamento general de protección de datos depende, o bien de que el responsable o el encargado del tratamiento esté establecido en la UE, o bien de que se traten datos de ciudadanos de la UE, incluso aunque el responsable o el encargado del tratamiento no esté establecido en el territorio de la UE[17], en cuyo caso deberán también designar un representante legal en la UE[18]. Desde la perspectiva de la protección de datos, es importante tener en cuenta que la ampliación del ámbito territorial tiene por objeto proporcionar una protección más amplia a los titulares de datos de la UE, independientemente del lugar en que esté establecida la empresa que trate sus datos.

Por lo tanto, aunque la desaparición de los criterios de ubicación podría representar una novedad en el ámbito del Derecho penal, no parece un cambio importante desde la perspectiva de la protección de datos. Además, el SEPD toma nota asimismo de que todavía se mantiene un vínculo con el territorio de la UE, ya que solo los proveedores de servicios en la Unión entran en el ámbito de aplicación de la propuesta, y el hecho de que las solicitudes solo puedan dirigirse en el marco de las investigaciones penales implica un vínculo con la UE (bien porque el delito se haya cometido en el territorio de un Estado miembro o bien porque la víctima o el autor del delito sea un ciudadano de un Estado miembro).

Si la desaparición de los criterios de ubicación debe aplicarse ahora en el Derecho penal, la cuestión más importante para el SEPD es cómo garantizar que esta evolución no sea perjudicial para la protección de datos y los derechos procesales penales de los interesados y los proveedores de servicios requeridos. Desde esta perspectiva, el SEPD reconoce que en la UE se han armonizado, al menos parcialmente, las garantías procesales y que éstas deben ser conformes con el Convenio Europeo de Derechos Humanos. Por ello se puede aducir que la desaparición de los criterios de ubicación probablemente tenga unas consecuencias más limitadas cuando la prueba se busque dentro de la UE, en comparación con la situación inversa en que las autoridades de terceros países soliciten datos a empresas establecidas en la UE, en las mismas condiciones enunciadas en el proyecto de Reglamento sobre las pruebas electrónicas. El SEPD está especialmente preocupado porque ello podría dar lugar a más situaciones problemáticas. En este contexto, las autoridades de un tercer país en el que se apliquen garantías procesales diferentes y potencialmente inferiores en el ámbito del Derecho penal podrían tener acceso a datos que estarían protegidos por salvaguardias adicionales en la UE. Desde este punto de vista, el SEPD recuerda su preocupación por la existencia de un doble rasero y el debilitamiento de los derechos fundamentales cuando los proveedores de servicios y los titulares de datos no se beneficien de las garantías procesales establecidas en el Derecho de la UE cuando la solicitud se presente desde un tercer país.

Por otra parte, como este nuevo criterio de competencia judicial «con independencia de la ubicación de los datos» se combina con un procedimiento basado principalmente en solicitudes directas de las autoridades competentes a los proveedores de servicios, al SEPD le preocupa que las garantías de protección de datos no puedan ser aplicadas por las empresas privadas que reciben las solicitudes y que no están obligadas por un instrumento jurídico como un TAJM, que tradicionalmente regulan los intercambios de datos entre autoridades judiciales y ofrecen garantías. En particular, en el contexto

[17] Véase el artículo 3, en particular el apartado 2.

[18] Véase el artículo 27

de los TAJM, las garantías mínimas de protección de datos implican, por ejemplo, obligaciones de confidencialidad y el principio de especificidad, que supone que los datos no serán tratados con otros fines.

El SEPD recuerda, por lo tanto, que al menos deben ser aplicables las garantías previstas en la Directiva 2016/680, especialmente respecto de las transmisiones de datos, y especialmente su artículo 39, en caso de que el proveedor de servicios esté establecido en un tercer país sin una decisión de adecuación en este ámbito. En particular, el SEPD subraya que esta disposición se refiere concretamente a la información de la autoridad de protección de datos competente en el Estado miembro de la autoridad de emisión de la orden y a la documentación de la transmisión, en particular la justificación de la ineficacia o inadecuación de una transmisión a la autoridad competente del tercer país.

4. El concepto de «proveedor de servicios» debe restringirse o complementarse con garantías adicionales de los derechos de los titulares de datos

Por lo que se refiere a los proveedores de servicios, el SEPD acoge con satisfacción la amplia definición, que permite incluir tanto los servicios de comunicación como los servicios de transmisión libre (OTT), puesto que todos estos servicios son funcionalmente equivalentes y, por lo tanto, las medidas previstas podrían tener un impacto similar sobre el derecho a la privacidad y el derecho al secreto de las comunicaciones, como se subraya en la declaración del GT29 y, anteriormente, en el Dictamen 01/2017 relativo a la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas. En efecto, la propuesta de Reglamento sobre las pruebas electrónicas abarca los proveedores de servicios que ofrecen servicios de comunicaciones electrónicas, según se definen en el artículo 2, punto 2, de la Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas; servicios de la sociedad de la información, tal como se definen en el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535, «para los que el almacenamiento de datos es un componente del servicio prestado al usuario, incluidas las redes sociales, los mercados en línea que facilitan las transacciones entre sus usuarios, y otros proveedores de servicios de alojamiento de datos» y servicios de asignación de nombres y números en internet, «como los registros de nombres de dominio de proveedores y de direcciones IP, los registradores de nombres de dominio y los servicios relacionados con la intimidad y la representación»[19].

Sin embargo, al ser, en el sentido de la propuesta de Reglamento, proveedor de servicios «toda persona física o jurídica que preste uno o más de los siguientes tipos de servicios», al SEPD le preocupa que este instrumento pueda abarcar tanto a los responsables como a los encargados del tratamiento de datos en el sentido del Reglamento general de protección de datos. En efecto, como la «oferta de servicios », tal como se define en el artículo 2, punto 3, del proyecto de Reglamento, permite que las personas físicas y jurídicas en uno o varios Estados miembros utilicen los servicios enumerados y tengan una estrecha vinculación con los Estados miembros en cuestión, están incluidas las actividades realizadas por un encargado para un responsable del tratamiento, tales como el almacenamiento de datos, por ejemplo.

[19] Artículo 2, punto 2, letra c), de la propuesta de Reglamento sobre las pruebas electrónicas.

Por tanto, el SEPD teme que, sin limitaciones a los proveedores de servicios que actúan como responsables del tratamiento en el sentido del Reglamento general de protección de datos, y sin ninguna obligación específica del encargado del tratamiento de notificar al responsable del tratamiento de datos cuando recibe una orden de conservación de datos, pueden eludirse los derechos de los titulares de datos. Este es especialmente el caso, puesto que en el contexto de posibles conflictos de obligaciones que impidan al destinatario cumplir las órdenes recibidas, el proyecto de Reglamento también alienta a las autoridades judiciales a dirigirse a la persona más adecuada, con independencia de las normas de protección de datos aplicables, en particular teniendo en cuenta que puede solicitarse cualquier dato y no solo los datos personales sujetos al Reglamento general de protección de datos[20].

De conformidad con el Reglamento general de protección de datos, el encargado del tratamiento solo actúa siguiendo las instrucciones dadas por el responsable del tratamiento. Por consiguiente, compete al responsable del tratamiento garantizar los derechos de los titulares de datos, y proporcionarles la información pertinente, en particular en lo que atañe a los destinatarios de sus datos, por ejemplo en el contexto del ejercicio de su derecho de acceso. El encargado del tratamiento no recibirá dichas solicitudes de los titulares de datos y no estará en condiciones de responder, a menos que se lo pida expresamente el responsable del tratamiento.

Por consiguiente, a menos que sus derechos hayan sido limitados en aplicación del Reglamento general de protección de datos, el SEPD subraya que los titulares de datos que se benefician de la aplicación del Reglamento general de protección de datos no podrán ejercer sus derechos de forma eficaz si el responsable del tratamiento no está en condiciones de proporcionar una información completa. El SEPD también señala que la probabilidad de falta de información es incluso mayor al no imponerse al encargado del tratamiento una obligación específica de informar al responsable del tratamiento cuando los datos solicitados se refieren a titulares de datos que no se benefician de la protección concedida por el Reglamento general de protección de datos. De hecho, las autoridades judiciales que solicitan los datos no tienen necesariamente la obligación de informar a los interesados de su tratamiento posterior en este caso. El SEPD pide, por consiguiente, que se restrinja el ámbito de aplicación a los responsables del tratamiento en el sentido del Reglamento general de protección de datos, o que se introduzca una disposición que aclare que si el proveedor de servicios al que se dirige la orden no es el responsable del tratamiento de datos, informará de ello al responsable del tratamiento.

5. Los conceptos de «establecimiento» y de «representante legal» en el contexto de estas propuestas deben distinguirse claramente de estos conceptos en el contexto del Reglamento general de protección de datos

Habida cuenta de la inaplicabilidad de los criterios de ubicación con respecto a los datos, los destinatarios de las órdenes de conservación y entrega de pruebas electrónicas en el ámbito de aplicación de la propuesta de Reglamento se limitan a los proveedores de servicios que prestan servicios en la Unión, con independencia de que estén establecidos en la UE o no, con la obligación de designar un representante legal con arreglo a las normas propuestas en el proyecto de Directiva.

[20] Véase el artículo 7, apartados 3 y 4.

Estos conceptos de «establecimiento» y de «representante legal» se definen, por lo tanto, en el proyecto de instrumentos.

El SEPD observa que estos conceptos figuran también en el contexto de otros instrumentos de la UE y, en particular, en el contexto del Reglamento general de protección de datos. Por consiguiente, deben facilitarse aclaraciones en cuanto a la definición y delimitación de estos conceptos en el contexto de las propuestas y en el contexto del Reglamento general de protección de datos.

a) Establecimiento

El SEPD también recuerda que el concepto de «establecimiento» en el contexto del proyecto de Reglamento no debe confundirse con este mismo concepto en el contexto del Reglamento general de protección de datos. De hecho, a efectos del proyecto de Reglamento, el concepto de establecimiento, tal como se define en el artículo 2, punto 4, es más amplio que el del Reglamento general de protección de datos, puesto que incluye el «ejercicio efectivo de una actividad económica por tiempo indefinido a través de una infraestructura estable a partir de la cual se realiza la actividad de prestación de servicios o de una infraestructura estable a partir de la cual se gestiona la actividad», con independencia de que el tratamiento de datos personales tenga lugar en el marco de las actividades de ese establecimiento. Por lo tanto, si el «establecimiento» en el sentido del Reglamento general de protección de datos queda, sin duda, incluido en la definición de establecimiento del proyecto de Reglamento, lo contrario podría no ser el caso.

El SEPD, por tanto, advierte que los establecimientos de los proveedores de servicios en el sentido de la propuesta de Reglamento no implican necesariamente que se cumplan las condiciones para la aplicación del Reglamento general de protección de datos, de conformidad con el artículo 3, apartado 1. En este contexto, se invita por lo tanto a los responsables y a los encargados del tratamiento a comprobar si la aplicabilidad del Reglamento general de protección de datos no se deriva del artículo 3, apartado 2, lo que implicaría la designación de un representante legal en la UE y la ausencia de un mecanismo de ventanilla única.

b) Representante legal

En su declaración, el GT29 hizo hincapié en que debe evitarse cualquier confusión entre la obligación de designar un representante legal con arreglo al artículo 27 del Reglamento general de protección de datos y el representante legal previsto en el proyecto de Reglamento sobre las pruebas electrónicas.

Con ocasión del proyecto de propuesta, el SEPD desea recordar estas recomendaciones y, en particular, subrayar que, en su opinión, el representante legal en el sentido de la propuesta de Directiva sobre la designación de representantes legales en el contexto de las pruebas electrónicas será designado en cualquier caso; tendrá funciones específicas, con independencia del mandato otorgado por el proveedor de servicios; estará facultado para responder a las solicitudes y para actuar en nombre del proveedor de servicios, y tendrá una responsabilidad mayor que el representante legal del Reglamento general de protección de datos.

Por otra parte, el SEPD insiste en que la obligación de designar un representante legal en cualquier caso en el marco de las propuestas sobre las pruebas electrónicas, tanto si el proveedor de servicios está establecido en la UE como si no; la posibilidad de designar varios representantes legales para el mismo proveedor en virtud del proyecto de Directiva sobre las pruebas electrónicas, y la obligación de notificar la designación del representante legal a las autoridades de los Estados miembros difieren del Reglamento general de protección de datos, que no dispone la obligación de notificar el

representante legal, excepciones a la designación ni la responsabilidad limitada del representante legal.

Por consiguiente, habida cuenta de las importantes diferencias en términos de función, responsabilidad y relación con los demás establecimientos del proveedor de servicios, en un caso, y del responsable o del encargado del tratamiento en el otro, el SEPD recomienda que, cuando un proveedor de servicios no esté establecido en la Unión Europea, pero esté sujeto tanto al Reglamento general de protección de datos con arreglo al artículo 3, apartado 2, como al Reglamento sobre las pruebas electrónicas, se designen dos representantes legales, cada uno de ellos con clara funciones distintas en función del instrumento sobre la base del cual ha sido designado.

6. Nuevas categorías de datos

La propuesta de Reglamento define las distintas categorías de datos en el artículo 2: los datos de los abonados, los datos relativos al acceso, los datos de transacciones y los datos de contenido. El considerando 20 de la propuesta de la Comisión específica además que «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.»

En este contexto, el SEPD destaca, en primer lugar, que las cuatro categorías de datos antes citadas deben considerarse datos personales de conformidad con la legislación europea sobre protección de datos, ya que contienen información relativa a una persona física identificada o identificable, ya se denomine al titular de datos «abonado» o «usuario» en la propuesta de Reglamento. Del mismo modo, hay que señalar que las «pruebas electrónicas», tal como se definen en el artículo 2, punto 5, de la propuesta de la Comisión abarcan las cuatro categorías de datos, por lo que se refieren a datos personales. Por lo tanto, en lugar de establecer las normas para el acceso a las pruebas, definidas y cualificadas en la legislación y los procedimientos judiciales nacionales, la propuesta de Reglamento establece nuevas condiciones sustantivas y procedimentales para el acceso a los datos personales.

Si la propuesta de Reglamento establece nuevas subcategorías de datos personales a las que se aplican distintas condiciones del procedimiento de acceso, el SEPD recuerda que, de conformidad con la jurisprudencia pertinente del TJUE, para demostrar la existencia de una injerencia en el derecho fundamental a la privacidad, carece de relevancia que la información relativa a la vida privada de que se trate sea sensible o que los interesados hayan sufrido molestias en modo alguno.

Por otra parte, el SEPD recuerda que, en relación con «los datos sin contenido», que incluyen los datos de los abonados, los datos relativos al acceso y los datos de transacciones en la propuesta de la Comisión, el Tribunal de Justicia de la Unión Europea ha declarado en su sentencia en los asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB* que los metadatos, como los datos de tráfico y de localización de datos, proporcionan medios para determinar el perfil de los interesados, información tan sensible, respecto del derecho a la privacidad, como el propio contenido de las comunicaciones[21].

[21] Sentencia del TJUE de 21 de diciembre de 2016, apartado 99.

Como ya se indicó en la declaración del GT29 sobre la protección de datos y los aspectos relativos a la privacidad del acceso transfronterizo a las pruebas electrónicas, de 29 de noviembre de 2017, el SEPD reitera sus dudas e inquietudes en lo que respecta a la delimitación actual entre datos «sin contenido» y datos de contenido, así como a las cuatro categorías de datos personales establecidas en la propuesta de Reglamento. En efecto, las cuatro categorías propuestas no parecen estar claramente delineadas y la definición de «datos relativos al acceso» sigue siendo vaga, en comparación con las demás categorías. El SEPD lamenta por lo tanto que la evaluación de impacto y la propuesta de la Comisión no justificaran con mayor fundamento el motivo de la creación de estas nuevas categorías de datos personales, y manifiesta su preocupación por los diferentes niveles de garantías relativas a las condiciones sustantivas y procedimentales para el acceso a las categorías de datos personales, especialmente por la dificultad práctica de determinar a qué categorías de datos pertenecen los datos solicitados en algunos casos. Por ejemplo, las direcciones IP podrían calificarse como datos de transacciones y datos de abonados.

En este contexto, el SEPD también recuerda que, en el considerando 14 de su propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (privacidad electrónica), la Comisión considera que «Los datos de comunicaciones electrónicas deben definirse de manera lo suficientemente amplia y tecnológicamente neutra como para incluir cualquier información relativa al contenido transmitido o intercambiado (contenido de las comunicaciones electrónicas) y la información relativa al usuario final de servicios de comunicaciones electrónicas que se haya tratado con el fin de transmitir, distribuir o permitir el intercambio de contenido de comunicaciones electrónicas; incluidos los datos para rastrear e identificar el origen y el destino de una comunicación, la localización geográfica y la fecha, hora, duración y tipo de comunicación.» Dado que el marco actual y futuro de la privacidad electrónica, así como las correspondientes limitaciones al derecho a la privacidad, se aplicarán a las normas que regulan el acceso de las autoridades policiales a las pruebas electrónicas, el SEPD recomienda que se incluya una definición más amplia de los datos de las comunicaciones electrónicas en la propuesta de Reglamento, con el fin de garantizar que las garantías y condiciones de acceso oportunas que se establezcan abarquen sistemáticamente tanto los datos «sin contenido» como los «datos de contenido».

7. Análisis de los procedimientos de las órdenes europeas de conservación y entrega de pruebas electrónicas

En términos generales, el procedimiento para remitir una orden de conservación o entrega de pruebas electrónicas parece ser la siguiente:

- La autoridad judicial competente - la autoridad de emisión -, dependiendo del tipo de datos solicitados y del tipo de orden, emite la orden con arreglo a las (escasas) condiciones enumeradas en los artículos 5 y 6 y la envía utilizando un certificado armonizado al representante legal del proveedor de servicios o de su establecimiento en la UE - el destinatario-.
- Tras la recepción del certificado, el destinatario debe ejecutar la orden, en el sentido de transmitir los datos en un plazo de diez días, o de seis horas en caso de emergencia, o conservarlos hasta sesenta días, a menos que resulte imposible hacerlo, porque el certificado esté incompleto, por causa de fuerza mayor, por imposibilidad *de facto* del destinatario o porque el destinatario se niegue a causa de un conflicto de obligaciones , ya sea con respecto

a los derechos fundamentales o los intereses fundamentales de un tercer país o por otros motivos.

- En caso de que el destinatario no cumpla la orden recibida sin alegar ningún motivo aceptado por la autoridad de emisión, se han previsto procedimientos para que las órdenes las ejecute una autoridad de ejecución competente del Estado miembro en el que el proveedor de servicios esté representado o establecido, salvo que existan motivos tasados de denegación y la autoridad de ejecución se oponga al reconocimiento o a la ejecución de la orden.
- En caso de que el destinatario alegue una objeción motivada contra la orden sobre la base de un conflicto de obligaciones, la autoridad de emisión deberá remitir el asunto al órgano jurisdiccional competente de su Estado miembro, que deberá evaluar el posible conflicto y mantener la orden en ausencia de conflicto. En caso de conflicto, la jurisdicción competente, o bien se dirigirá a las autoridades centrales del tercer país, a través de sus autoridades centrales nacionales, con un plazo de quince días para responder, prorrogable por treinta días, previa solicitud motivada, en caso de conflicto de obligaciones con respecto a los derechos fundamentales o los intereses fundamentales de un tercer país, o bien determinará por sí misma si mantiene o retira la orden por motivos distintos de los alegados por el destinatario para negarse a su cumplimiento.
- Sin perjuicio de las vías de recurso disponibles con arreglo al Reglamento general de protección de datos y las LED, las personas cuyos datos se obtuvieron a través de una orden de entrega también tendrán derecho a vías de recurso efectivas contra esa orden.

El SEPD ha evaluado los procedimientos previstos y las garantías dispuestas en la propuesta de Reglamento para las diferentes etapas, y sobre cada uno de los aspectos que se presentan a continuación recomienda las salvaguardias y modificaciones siguientes.

a) Deben elevarse los umbrales para emitir órdenes y las órdenes deben ser emitidas o autorizadas por los órganos jurisdiccionales

Por lo que se refiere a las condiciones de emisión de las órdenes, el SEPD acoge con satisfacción el principio de mayores garantías para el acceso a los datos de transacciones o de contenido. Observa, no obstante, que, dada la ausencia de una armonización completa de las sanciones penales entre los Estados miembros, la referencia a los «delitos punibles en el Estado emisor con una pena máxima de privación de libertad de tres años»[22] implica diferentes umbrales y discrepancias en la protección de los datos de los interesados dentro de la UE.

Por otra parte, el SEPD destaca que, especialmente por la amplia definición del concepto de datos de los abonados, el umbral fijado parece más bien bajo para las órdenes de conservación y entrega relativas a los datos de los abonados o los datos relativos al acceso, puesto que todas las infracciones penales pueden justificar, en principio, la emisión de dichas órdenes. Del mismo modo, las autoridades autorizadas a emitir dichas órdenes son más limitadas para la emisión de órdenes de entrega de datos de transacciones o de contenido que para la emisión de órdenes de conservación o entrega de datos de los abonados o datos relativos al acceso, porque los fiscales solo pueden emitir o autorizar estas últimas, mientras que cualquier juez, órgano jurisdiccional o juez de instrucción puede emitir o autorizar cualquier orden.

[22] Véase el artículo 5, apartado 4, letra a).

En particular, el SEPD lamenta que el umbral más bajo que contempla la posibilidad de que las autoridades policiales soliciten el acceso a datos de los abonados o a datos relativos al acceso por cualquier infracción penal se basa en una lectura *a contrario* de la jurisprudencia del TJUE (que se centra en los demás datos) para hacer distinciones entre las garantías que se ofrecen. En efecto, el TJUE hace especialmente hincapié en que, en el caso de los datos de tráfico y de localización, el acceso de las autoridades competentes estará restringido exclusivamente a la lucha contra los delitos graves[23]. El SEPD podría comprender que la propuesta contemple la posibilidad de solicitar el acceso a información muy básica que solo permita identificar a una persona sin revelar cualesquiera datos de comunicaciones sin la autorización previa de un órgano jurisdiccional. Sin embargo, lamenta la amplia lectura *a contrario* de esta sentencia por parte de la Comisión y pide mayores garantías a fin de restringir las posibilidades de acceso a otros datos de los abonados y datos relativos al acceso. El SEPD propone restringir el acceso a dichos datos a una lista de delitos que figure en el proyecto de Reglamento, o, al menos, a los «delitos graves», especialmente teniendo en cuenta el bajo umbral de autorización previa previsto para estos datos.

Además, el SEPD subraya que esta lectura *a contrario* también da lugar a que la propuesta abra la posibilidad de que los fiscales emitan o autoricen la emisión de órdenes. El SEPD opina que, salvo en el caso de las solicitudes relativas a información muy básica que solo permita identificar a una persona sin revelar datos de comunicaciones, esto constituye un retroceso con respecto a la jurisprudencia del TJUE sobre el acceso a los datos de comunicaciones. De hecho, en su jurisprudencia sobre el acceso a los datos de comunicaciones a efectos policiales, el TJUE ha limitado la posibilidad de facilitar el acceso, entre otros criterios, y «salvo en casos de urgencia debidamente justificados»[24], a un «control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo», «a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos.»[25]

El SEPD recuerda que el concepto de «órgano jurisdiccional» es un concepto autónomo del Derecho de la Unión, y que el Tribunal de Justicia ha subrayado y recordado constantemente los criterios que deben cumplirse para ser considerado como un órgano jurisdiccional, incluidos los criterios de independencia[26], que no parece ser el caso de los fiscales, como recuerda también el Tribunal Europeo de Derechos Humanos en su jurisprudencia[27].

Por lo tanto, los artículos 4, apartado 1, letras a) y b), y apartado 3, letras a) y b), dan lugar a procedimientos en los que se aplicarán considerablemente menos garantías a los datos de los abonados y los datos relativos al acceso, puesto que un fiscal por sí solo podrá solicitar los datos, sin ningún otro control de la autoridad del Estado en que los datos se solicitan o de la autoridad del lugar de residencia del representante legal de la empresa requerida, ni el control de una autoridad administrativa independiente.

Además, el SEPD toma nota de la denominada garantía adicional prevista en el artículo 5, apartado 2, que limita la posibilidad de emitir una orden de entrega cuando esté prevista una medida similar para la misma infracción penal en una situación comparable a nivel nacional. No obstante, advierte contra los efectos contraproducentes de dicha disposición: en lugar de proporcionar garantías adicionales, parece un estímulo para que los Estados miembros amplíen sus posibilidades de solicitar

[23] Véase el asunto 203/15, apartado 125.
[24] Véase el asunto 203/15, apartado 120.
[25] Véanse los asuntos acumulados C 293/12 y C 594/12, apartado 62.
[26] Véase, por ejemplo, el asunto C 203/14.
[27] Véase, por ejemplo, *Moulin c/Francia*, de 23/11/2010.

la entrega de datos de los abonados y datos relativos al acceso con el objeto de asegurarse la emisión de órdenes de entrega de conformidad con el presente Reglamento.

b) Los plazos para proporcionar los datos deben justificarse

El SEPD señala que las de órdenes europeas de entrega de datos deben responderse en un plazo máximo de diez días a partir de la recepción del certificado, a menos que la autoridad de emisión alegue motivos para su comunicación en un plazo menor, y, a más tardar, en el plazo de seis horas en los casos de urgencia, de conformidad con el artículo 9, apartados 1 y 2.

Sin embargo, el SEPD observa la ausencia de criterios para la definición de la obligación impuesta a las autoridades de demostrar la urgencia para la entrega de los datos, incluso *a posteriori* a fin de permitir un posible control de la utilización de este procedimiento acelerado, mientras que el plazo de seis horas probablemente implique un control muy liviano antes de la entrega de los datos, si no la ausencia de cualquier tipo de control por parte del proveedor de servicios. De hecho, la evaluación de impacto subraya la necesidad de que las autoridades competentes tengan acceso a los datos de manera oportuna. No obstante, los ejemplos que se aportan en la evaluación de impacto se refieren todos ellos a las pruebas necesarias en caso de delitos graves (actos de terrorismo con rehenes, situaciones de abuso sexual de menores), pero la justificación basada en la volatilidad de las pruebas no parece ser válida cuando no hay otra urgencia distinta que esa potencial volatilidad de los datos. Además, la volatilidad de los datos no proporciona ninguna justificación adicional a la proporcionalidad para tener acceso a los datos con menos garantías en estas situaciones en las que no existe otra urgencia que la volatilidad de los datos.

Además, el SEPD duda de la necesidad de fijar un plazo de seis horas al mismo tiempo que se dispone que este plazo no se aplicará hasta que la autoridad emisora ofrezca aclaraciones adicionales «en un plazo de cinco días» en el caso de que el proveedor de servicios no pueda cumplir su obligación.

El SEPD pide, por tanto, elementos adicionales en la evaluación de impacto que justifiquen la necesidad de estos plazos en los casos en los que el delito cometido o enjuiciado no sea grave, y a menos que se proporcionen tales elementos detallados, criterios explícitos para justificar la urgencia en caso de que se emitan las órdenes. Podría preverse, por ejemplo, el mismo modelo que la Directiva sobre la OEI, que establece un plazo más corto cuando esté justificado por «los plazos procesales, la gravedad del delito u otras circunstancias particularmente urgentes» (artículo 12, apartado 2), o un plazo de 24 horas para tomar una decisión sobre las medidas provisionales (artículo 32, apartado 2). De hecho, la evaluación de impacto de la propuesta de Reglamento no proporciona elementos detallados que justifiquen por qué estos plazos no son eficientes, al subrayarse como único elemento que el número de solicitudes enviadas sobrecargue de trabajo a las autoridades judiciales de modo que no puedan respetar los plazos.

c) Las órdenes europeas de conservación y entrega de datos no deberán utilizarse para solicitar datos de interesados de otro Estado miembro sin informar al menos a las autoridades competentes de ese Estado miembro, en particular para los datos de contenido 17

El SEPD recuerda que en los instrumentos ya existentes se dispone la cooperación judicial y, por lo tanto, garantías adicionales, en particular para controlar la necesidad y la proporcionalidad de las solicitudes, y subraya que estas garantías están más que nunca justificadas cuando se solicitan datos de contenido que implican más limitaciones de los derechos de los interesados a la protección de sus datos personales y de su intimidad. A este respecto, el SEPD recuerda que la Directiva sobre la OEI establece, asimismo, la posibilidad de interceptar las telecomunicaciones con la asistencia técnica de

otro Estado miembro (véase el artículo 30), así como la obligación de notificar toda interceptación de datos a la autoridad competente de otro Estado miembro en los casos en que la asistencia no sea necesaria porque el interesado se halle o vaya a estar en el territorio del Estado miembro de que se trate (véase el artículo 31).

El SEPD no encuentra ninguna justificación para que el procedimiento previsto en el proyecto de Reglamento sobre las pruebas electrónicas permita la entrega de datos de contenido sin participación alguna al menos de las autoridades competentes del Estado miembro en el que se halle el interesado.

d) Las órdenes europeas de conservación de datos no deberán utilizarse para eludir las obligaciones de conservación de datos de los proveedores de servicios

El SEPD toma nota de que la principal finalidad de las órdenes de conservación de datos es impedir que los datos se borren.

Aunque el SEPD reconoce que puede ser necesario y proporcionado en algunos casos, lamenta la falta de garantías para la emisión de dichas órdenes. En particular, el SEPD recomienda que cuando las órdenes de conservación se refieran a datos específicos, cuando el proyecto parezca permitir solicitudes amplias y cuando se emitan órdenes para datos que esté previsto borrar de conformidad con el principio de conservación de datos, la orden no podrá en ningún caso servir de base para que el proveedor de servicios trate los datos después de la fecha inicial de supresión. En otras palabras, los datos deben «congelarse».

Además, el vínculo entre la orden de conservación de datos y la solicitud subsiguiente de entrega de datos, ya sea a través de una orden europea de entrega de datos, una solicitud de OEI o una petición de asistencia judicial mutua, debe reforzarse a fin de garantizar que solo se emitan órdenes de conservación de datos cuando la otra solicitud sea cierta (y no solo se contemple como una posibilidad), y que cuando la otra solicitud sea denegada, la orden de conservación de datos también lo sea, sin tener que esperar sesenta días[28] si la solicitud subsiguiente es denegada antes.

e) Confidencialidad e información a los usuarios

El SEPD toma nota de que se ha introducido en el proyecto de Reglamento un artículo específico[29] sobre la confidencialidad de las órdenes. Con el objeto de evitar cualquier confusión y malentendido con el derecho a la protección de datos, el SEPD recuerda que, aunque el Reglamento general de protección de datos establece que las limitaciones a los derechos de los interesados a fin de garantizar la prevención, la investigación, la detección o el enjuiciamiento de las infracciones penales deben disponerse por ley y, por lo tanto, ser públicamente accesibles[30] y que estas medidas legislativas deben contener disposiciones específicas en cuanto al derecho de los interesados a ser informados sobre la restricción, salvo cuando pueda ser perjudicial a los fines de esta[31], no dispone la obligación de informar individualmente a los interesados de cada solicitud de acceso por parte de las autoridades policiales.

---

[28] Véase el artículo 10, apartado 1.
[29] Véase el artículo 11.
[30] Véase el artículo 23, apartado 1, letra d).
[31] Véase el artículo 23, apartado 2, letra h).

No obstante, mientras tanto, el SEPD recuerda que la Directiva sobre protección de datos establece este derecho de información de los interesados por parte de las propias autoridades competentes, a menos que este derecho haya sido restringido, para cualquier interesado, sin limitarlo únicamente a los interesados que residan en el territorio de la UE.

f) Procedimiento para la ejecución de una orden cuando el proveedor de servicios se niegue a ejecutarla

El SEPD señala que el artículo 14 de la propuesta de Reglamento establece un procedimiento para garantizar la ejecución de una orden cuando el destinatario no la cumpla, basado en la cooperación judicial entre la autoridad de emisión y la autoridad competente en el Estado de ejecución.

No obstante, parece que este procedimiento no permite a la autoridad de ejecución negarse a ejecutar la orden transmitida por otros motivos distintos de los de meramente procedimentales (lo mismo que el destinatario, principalmente por falta de información o imposibilidad material de proporcionar los datos), porque los datos en cuestión están protegidos por una inmunidad o privilegio en virtud de su Derecho interno o porque su revelación puede afectar a sus intereses fundamentales, como la seguridad y la defensa nacionales[32].

El SEPD reitera, por lo tanto, su preocupación por lo que se refiere a la eliminación de toda doble comprobación por la autoridad competente receptora de la orden transmitida, en comparación con los otros instrumentos. Incluso el motivo de negarse a ejecutar una orden que violaría la Carta parece superior al umbral clásico relativo a la vulneración de los derechos fundamentales del interesado. Por consiguiente, siguiendo el ejemplo de la orden de detención europea, que prevé motivos obligatorios y opcionales de denegación o, al menos, de la Directiva sobre la OEI, que establece que la presunción general de que «la creación de un espacio de libertad, seguridad y justicia en la Unión se basa en la confianza mutua y en una presunción del respeto, por parte de los demás Estados miembros, del Derecho de la Unión y, en particular, de los derechos fundamentales» es refutable[33], el proyecto de Reglamento debe, al menos, prever la excepción mínima clásica de que si existen motivos fundados para creer que la ejecución de una orden implicaría una violación de un derecho fundamental del interesado y que el Estado de ejecución incumpliría sus obligaciones relativas a la protección de los derechos fundamentales reconocidos en la Carta, la ejecución de la orden debe ser denegada.

g) Ejecución de órdenes y conflicto de obligaciones en virtud de las leyes de terceros países (artículos 15 y 16)

El SEPD acoge con satisfacción la posibilidad prevista en el proyecto de Reglamento de que los destinatarios rehúsen la ejecución de una orden que entre en conflicto con derechos fundamentales, ya que aporta garantías en caso de conflicto de obligaciones legales. También considera esencial que la propuesta prevea la consulta de las autoridades de terceros países, al menos cuando surja un conflicto, así como la obligación de suspender la orden cuando una autoridad de un tercer país formule una objeción.

Por lo tanto, el procedimiento previsto para negarse a ejecutar una orden con motivo de un conflicto de obligaciones en virtud de las leyes de terceros países debe mejorarse considerablemente.

En primer lugar, el SEPD observa que el proyecto de Reglamento encomienda a una empresa privada, como destinataria de una orden de entrega de datos, la evaluación de si dicha orden entra en

[32] Véase el artículo 14, apartado 2.
[33] Véase el considerando 19 de la Directiva sobre la OEI.

conflicto con la legislación aplicable de un tercer país que prohíbe la comunicación de los datos solicitados. La empresa tiene que formular una objeción motivada, incluidos todos los detalles pertinentes de la legislación del tercer país, su aplicabilidad al caso en cuestión y la naturaleza del conflicto de obligaciones .

Y lo que es más importante, al SEPD le preocupa que cuando se formule dicha objeción, el órgano jurisdiccional competente del Estado miembro de la autoridad emisora solo evalúe si existe un conflicto o no, ya que solo cuando el órgano jurisdiccional constate la existencia de un conflicto deberá ponerse en contacto con las autoridades del tercer país. El órgano jurisdiccional competente de la UE tiene competencia para interpretar de manera concluyente la ley de un tercer país en este contexto, sin ser un especialista en la materia. El SEPD considera que la obligación de consultar a las autoridades competentes del tercer país es, por lo tanto, demasiado limitada en la propuesta actual. En el ámbito de la protección de datos, el SEPD llama la atención del legislador hacia el hecho de que, en caso de que el órgano jurisdiccional competente de un tercer país interprete el Reglamento general de protección de datos para evaluar si entra en conflicto con sus propios requisitos, las autoridades de protección de datos de la UE y los órganos jurisdiccionales competentes seguirán siendo competentes para evaluar la legalidad de la transmisión sobre la base de una sentencia de un órgano jurisdiccional o una decisión de una autoridad administrativa de un tercer país que exijan una transmisión o comunicación de datos personales dentro del ámbito de aplicación del Reglamento general de protección de datos[34].

Además, el SEPD subraya que la evaluación de la legislación del tercer país por el órgano jurisdiccional competente del Estado requirente de la UE debe basarse en elementos objetivos y manifiesta su preocupación por los criterios que debe tener en cuenta el órgano jurisdiccional competente a la hora de evaluar la legislación del tercer país con arreglo al artículo 15, apartado 4, y el artículo 16, apartado 5, letra a), de la propuesta de Reglamento. En efecto, el órgano jurisdiccional debería valorar el hecho de que «en lugar de proteger los derechos fundamentales o los intereses fundamentales del país tercero relacionados con la seguridad y la defensa nacionales», el Derecho del país tercero «pretende manifiestamente proteger otros intereses o tiene como objetivo proteger actividades ilegales frente a requerimientos de las autoridades policiales o judiciales en el contexto de investigaciones penales» o «el interés protegido por la legislación pertinente del país tercero, incluido el interés del país tercero en impedir la revelación de los datos». Por ejemplo, si bien, en principio, esta evaluación debería exigir una valoración de pruebas teniendo en cuenta toda la información disponible, dado el impacto potencial de una decisión de este tipo, al menos, la expresión («... tiene como objetivo») parece poco clara y debería adaptarse («tiene el propósito/la finalidad»).

El SEPD lamenta que el único caso en que las autoridades de un tercer país serían consultadas y podrían oponerse a la ejecución de una orden, sería aquel en que el órgano jurisdiccional competente de la UE considerara que existe un conflicto pertinente, transmitiera todos los elementos a las autoridades centrales del tercer país de que se trate y estas se opusieran dentro de un ajustado plazo máximo cincuenta días (quince días, que podrían prorrogarse por treinta días más, y después un último recordatorio con cinco días adicionales). En todos los demás casos, el órgano jurisdiccional competente estaría en condiciones de mantener la orden de entrega de datos e imponer una sanción pecuniaria al proveedor de servicios por oponerse a la ejecución de la orden. Por tanto, el SEPD está preocupado por el hecho de que los órganos jurisdiccionales competentes de la UE no tengan la obligación de consultar a las autoridades competentes de los terceros países

[34] Véase el artículo 48 del Reglamento general de protección de datos.

afectados a fin de asegurarse de que el procedimiento garantizará de forma más sistemática que los argumentos de ambas partes se tomarán en consideración y mostrar más respeto a las leyes de terceros países.

Como ya se destacó en la declaración del GT29 y anteriormente, el SEPD recuerda que se debe prestar especial atención a la adopción por parte de los terceros países de instrumentos similares que puedan afectar a los derechos de los titulares de los datos y al derecho a la intimidad en la UE, especialmente al riesgo de que instrumentos similares pudieran entrar en conflicto directo con la legislación europea sobre protección de datos.

Además, el SEPD subraya que el órgano jurisdiccional competente del Estado miembro de la autoridad de emisión puede que no sea incluso el órgano jurisdiccional competente para la ejecución de la orden prevista en el artículo 14 del proyecto de Reglamento, lo que podría aumentar el riesgo de conflicto de procedimientos y la falta de controles en una situación de conflicto de leyes. Ello se deriva del hecho de que, en algunos casos, tres Estados miembros podrían estar implicados: la autoridad que emite la orden, el tercer país del proveedor del servicio y el Estado miembro de residencia del representante legal del proveedor de servicios en la UE, donde la orden debe ejecutarse. Por lo tanto, tras el procedimiento previsto actualmente, el órgano jurisdiccional de la autoridad requirente en el Estado miembro **A** podría hacer su propia interpretación de la ley del tercer país **B** del proveedor de servicios, sin recabar la opinión de las autoridades de ese tercer país (aunque se hubieran opuesto a la orden), y solicitar a un órgano jurisdiccional de otro Estado miembro de la UE **C** que ejecute su decisión sin posibilidad de oposición.

Además, el SEPD también acoge favorablemente la introducción de normas específicas de recurso contra las órdenes de entrega de datos, además de las sanciones previstas en el Reglamento general de protección de datos y en la Directiva relativa a la protección de las personas físicas en el ámbito penal. El GT29 ya pidió tales garantías en su declaración anterior. No obstante, el SEPD lamenta que dichas vías de recurso no estén también previstas contra las órdenes de conservación de datos, puesto que estas órdenes pueden también dar lugar a restricciones de los derechos fundamentales de las personas cuyos datos se conservan. En efecto, las órdenes de conservación de datos pueden tener el efecto de conservar los datos durante más tiempo del previsto de acuerdo con las normas de protección de datos. Por lo tanto, en sí misma, la orden de conservación de datos supone una restricción de los derechos fundamentales del interesado, cuya justificación debe ser objeto de revisión y de recursos específicos, especialmente en los casos en que la orden de conservación de datos se haya emitido junto con una orden de entrega de datos. Según recomendó el GT29 en su declaración, deben disponerse vías de recurso al menos equivalentes a las existentes en un caso nacional.

h) Seguridad de las transmisiones de datos en respuesta a una orden

El SEPD toma nota de que el proyecto de Reglamento solo contempla que las órdenes se dirijan a destinatarios en la Unión Europea y, por lo tanto, no prevé ningún canal de distribución específico para la transmisión de datos entre destinatarios y proveedores de servicios situados fuera de la Unión Europea.

Aunque el SEPD acoge con satisfacción la ausencia de nuevas excepciones al marco general de la UE para la protección de datos, recuerda que cualquier orden enviada a un destinatario que implique una transmisión fuera de la UE tendrá que respetar el marco legal establecido por el Reglamento general de protección de datos. En efecto, la elusión del marco jurídico de cooperación judicial, que dispone garantías de protección de los datos que deben respetarse, no debe traducirse también en la

elusión de la transmisión de datos por parte de los destinatarios de las órdenes de conservación o entrega de datos en su cumplimiento.

Además, aunque el SEPD acoge con satisfacción la falta de una disposición que obligue a descifrar los datos cifrados[35], le preocupa el hecho de que las propuestas no prevén ningún requisito específico para que los destinatarios evalúen la autenticidad de los datos entregados, subraya que esta evaluación es también un valor añadido de los instrumentos tradicionales basados en la cooperación judicial y advierte contra el aumento de los riesgos para los interesados en ausencia de una evaluación de este tipo.

Conclusiones

Sobre la base de esta evaluación, el SEPD desea formular las siguientes recomendaciones a los colegisladores:

1) La base jurídica del Reglamento debe ser el artículo 82, apartado 1, del TFUE.
2) Debe demostrarse mejor la necesidad de un nuevo instrumento en comparación con la actual Directiva sobre la OEI o los TAJM, en particular con un análisis detallado de medios menos invasivos de los derechos fundamentales, como modificaciones de los instrumentos existentes o la limitación del ámbito de aplicación de este instrumento a las órdenes de conservación de datos en combinación con otros procedimientos para solicitar el acceso a los datos.
3) El Reglamento debe fijar un plazo más largo para permitir que el proveedor de servicios que ejecuta la orden garantice el respeto de las garantías de protección de los derechos fundamentales.
4) Debe mantenerse el principio de doble tipificación, especialmente si se abandona el criterio de ubicación de los datos a fin de mantener la obligación de tener en cuenta las salvaguardias previstas en ambos Estados afectados (el Estado de la autoridad requirente y el Estado de residencia del proveedor de servicios).
5) El ámbito de aplicación del Reglamento debe limitarse a los responsables del tratamiento de los datos en el sentido del Reglamento general de protección de datos o debe incluir una disposición que establezca que en el caso de que el proveedor de servicios requerido no sea el responsable del tratamiento de los datos, sino el encargado del tratamiento, este último esté obligado a informar al responsable del tratamiento.
6) El Reglamento debe incluir garantías relativas a las transmisiones de datos en el caso de que el proveedor de servicios esté establecido en un tercer país sin una decisión de adecuación en este ámbito, o remitirse a la Directiva 2016/680 para que estas garantías sean aplicables.
7) Dado que la designación obligatoria de un representante legal difiere del Reglamento general de protección de datos, el Reglamento debe precisar que el representante legal designado en virtud del Reglamento sobre las pruebas electrónicas debe ser distinto del designado con arreglo al artículo 3, apartado 2, del Reglamento general de protección de datos.
8) El Reglamento debe contener una definición más amplia de los datos de comunicaciones electrónicas a fin de garantizar que se establezcan las garantías y las condiciones de acceso adecuadas, tanto a los datos de contenido como a los datos sin contenido.
9) El Reglamento debe aumentar los umbrales para la emisión de órdenes y las órdenes deben ser emitidas o autorizadas por los órganos jurisdiccionales, a excepción de los datos de los abonados, a condición de que la definición de esta categoría de datos se reduzca

[35] Véase el considerando 19 y la página 240 de la evaluación de impacto.

drásticamente a una información muy básica que solo permita identificar a una persona sin que ello implique el acceso a datos de comunicaciones.

10) El Reglamento debe restringir el acceso a los datos de los abonados y a los datos relativos al acceso a una lista de infracciones penales estrictamente establecido o, al menos, a los «delitos graves».
11) El plazo para proporcionar los datos, especialmente en caso de urgencia, debe justificarse mejor en el Reglamento, y la posibilidad de utilizar un procedimiento acelerado de seis horas debería incluir la obligación de pedir a las autoridades que demuestren la urgencia que desencadena la utilización de este procedimiento, incluso *a posteriori*, con el fin de permitir un control de la utilización de tales facultades excepcionales.
12) Debe abandonarse el procedimiento que permite la entrega de datos de contenido sin la intervención de las autoridades competentes del Estado miembro en el que se halla el titular de los datos.
13) Deben mejorarse en el Reglamento las garantías concurrentes a la emisión de las órdenes de conservación de datos.
14) El Reglamento debe incluir al menos la excepción clásica mínima de que si existen motivos fundados para creer que la ejecución de una orden implicaría una violación de un derecho fundamental del interesado que induciría al Estado de ejecución a incumplir sus obligaciones respecto de la protección de los derechos fundamentales reconocidos en la Carta, debe rehusarse la ejecución de la orden.
15) El Reglamento debe disponer una amplia obligación de consulta de las autoridades competentes del tercer país de residencia del proveedor de servicios que proporcione los datos en caso de conflicto de leyes a fin de evitar interpretaciones subjetivas de un único órgano jurisdiccional.
16) La validez y duración de las órdenes de conservación de datos deben estar más vinculadas a las órdenes de entrega que las acompañen.
17) Debe garantizarse mejor la seguridad de la transmisión de datos.
18) Debe preverse la verificación de la autenticidad de los datos, en particular cuando puedan facilitarse datos cifrados.

Por el Supervisor Europeo de Protección de Datos

El Presidente

(Andrea Jelinek)