Declaración 2/2021 sobre el nuevo proyecto de disposiciones del Segundo Protocolo adicional al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest)

Adoptada el 2 de febrero de 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

El Comité Europeo de Protección de Datos (CEPD) ha adoptado la siguiente declaración:

Observaciones preliminares y contexto de la declaración del CEPD

El Comité Europeo de Protección de Datos (CEPD) y las autoridades de protección de datos de la UE están siguiendo de cerca el desarrollo del Segundo Protocolo adicional al Convenio de Budapest y han contribuido periódicamente a la consulta del Consejo de Europa, como la «conferencia Octopus» de carácter anual. En noviembre de 2019, el CEPD publicó también su última contribución a la consulta sobre un proyecto de Segundo Protocolo adicional[1], indicando que seguía estando «disponible para nuevas contribuciones» y pidió «una participación temprana y más proactiva de las autoridades de protección de datos en la preparación de estas disposiciones específicas, a fin de garantizar una comprensión y una consideración óptimas de las salvaguardias de protección de datos»[2].

Tras la publicación del nuevo proyecto de disposiciones del Segundo Protocolo adicional al Convenio de Budapest[3], el CEPD desea aportar una vez más una contribución experta y constructiva con vistas a garantizar que las consideraciones relativas a la protección de datos se tengan debidamente en cuenta en el proceso general de redacción del Protocolo adicional, teniendo en cuenta que las

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf
[2] El CEPD mantiene las posiciones y recomendaciones expresadas en esta contribución anterior y considera pertinente reformular los principios fundamentales a la luz de los últimos avances y nuevos proyectos de disposiciones publicados.
[3] https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations

reuniones dedicadas a la preparación del Protocolo adicional se celebran a puerta cerrada y que la participación directa de las autoridades de protección de datos en el proceso de redacción no se ha previsto en el mandato del T-CY[4].

El CEPD considera, además, que es probable que las disposiciones arriba mencionadas afecten a las condiciones de fondo y de procedimiento para el acceso a los datos personales en la UE, incluidas las derivadas de las solicitudes de autoridades de terceros países, haciéndose eco, por tanto, de los debates en curso a escala de la UE y de las iniciativas legislativas conexas que actualmente están siendo examinadas por los colegisladores[5]. Por lo tanto, el CEPD pide a la Comisión Europea y al Parlamento Europeo, así como a los Estados miembros de la UE y a los Parlamentos nacionales, que velen por que las negociaciones en curso sean objeto de un examen minucioso a fin de garantizar la plena coherencia del Segundo Proyecto de Protocolo adicional con el acervo de la UE, en particular en el ámbito de la protección de datos personales.

El acceso a los datos personales en todas las jurisdicciones ya ha sido abordado en el pasado por las autoridades de protección de datos de la UE en diversas posiciones y dictámenes, y el CEPD desea recordar una vez más, en particular, los comentarios del Grupo de Trabajo del Artículo 29 sobre la cuestión del acceso directo de las autoridades policiales de terceros países a los datos almacenados en otra jurisdicción, tal como se propone en el proyecto de elementos de un Protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia[6], así como su declaración sobre los aspectos de protección de datos y privacidad del acceso transfronterizo a las pruebas electrónicas[7]. El Supervisor Europeo de Protección de Datos ha emitido el Dictamen 3/2019 sobre el mandato para la participación de la Comisión en las negociaciones[8], así como el Dictamen 7/2019 sobre propuestas relativas a las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[9]. Estas contribuciones también se basan en el Dictamen 23/2018 del CEPD sobre las propuestas de la Comisión sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal[10].

El CEPD sigue siendo plenamente consciente de que las situaciones en las que las autoridades judiciales y policiales se enfrentan a una «situación transfronteriza» con respecto al acceso a los datos personales como parte de sus investigaciones pueden ser una realidad difícil y reconoce el objetivo legítimo de mejorar la cooperación internacional en materia de ciberdelincuencia y el acceso a la información. Al mismo tiempo, el CEPD reitera que deben garantizarse la protección de los datos personales y la seguridad jurídica, contribuyendo así al objetivo de establecer mecanismos sostenibles para el intercambio de datos personales con terceros países con fines policiales, que sean plenamente compatibles con los Tratados de la UE y la Carta de los Derechos Fundamentales de la UE. Además, el CEPD considera esencial enmarcar la preparación del Protocolo adicional en el contexto de los valores

[4] Mandato para la Preparación de un Segundo Proyecto de Protocolo adicional del Convenio de Budapest sobre la Ciberdelincuencia, aprobado por el 17.º Pleno del T-CY el 8 de junio de 2017, T-CY (2017) 3.
[5] En particular, pero no exclusivamente, los debates relativos a las propuestas de la Comisión sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.
[6] Observaciones del Grupo de Trabajo del Artículo 29 sobre la cuestión del acceso directo de las autoridades policiales de terceros países a los datos almacenados en otra jurisdicción, tal como se propone en el proyecto de elementos para un Protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia, de 5 de diciembre de 2013.
[7] Declaración del Grupo de Trabajo del Artículo 29 sobre los aspectos de protección de datos y privacidad del acceso transfronterizo a pruebas electrónicas, de 29 de noviembre de 2017.
[8] Dictamen del CEPD 3/2019 relativo a la participación en las negociaciones con vistas a un Segundo Protocolo adicional al Convenio de Budapest sobre Ciberdelincuencia.
[9] Dictamen del SEPD 7/2019 sobre las propuestas relativas a las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.
[10] Dictamen 23/2018 del CEPD adoptado el 26 de septiembre de 2018 sobre las propuestas de la Comisión sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

y principios fundamentales del Consejo de Europa, en particular los derechos humanos y el Estado de Derecho.

En relación con el «acceso directo transfronterizo a los datos informáticos almacenados», de conformidad con el artículo 32, letra b), del Convenio de Budapest, el CEPD reitera, en particular, que normalmente un responsable del tratamiento de datos solo puede revelar datos previa presentación de una autorización judicial o una orden judicial o de cualquier documento que justifique la necesidad de acceder a los datos y que haga referencia a la base jurídica pertinente para dicho acceso, presentada por una autoridad policial nacional con arreglo a su legislación nacional que especifique la finalidad para la que se requieren los datos.

Dado que el Convenio de Budapest, así como cualquiera de sus Protocolos adicionales, son instrumentos internacionales vinculantes, el CEPD subraya que, de conformidad con la jurisprudencia del TJUE, «las obligaciones impuestas por un acuerdo internacional no pueden tener por efecto perjudicar los principios constitucionales del Tratado CE, entre los que figura el principio según el cual todos los actos comunitarios deben respetar los derechos fundamentales, pues el respeto de esos derechos constituye un requisito de legalidad de dichos actos»[11]. Por lo tanto, es esencial que las partes negociadoras de la UE garanticen que las disposiciones establecidas en el Protocolo adicional se ajustan al acervo de la UE en el ámbito de la protección de datos, a fin de garantizar su compatibilidad con el Derecho primario y secundario de la UE.

Teniendo en cuenta el calendario del proceso de consulta, la contribución del CEPD se centrará en una evaluación preliminar del nuevo proyecto de disposiciones del Segundo Protocolo adicional al Convenio de Budapest que no hayan sido objeto de consultas previas con las partes interesadas:

- Equipos conjuntos de investigación e investigaciones conjuntas
- Revelación rápida de los datos informáticos almacenados en caso de emergencia
- Solicitud de información sobre el registro de nombres de dominio

Una vez más, el CEPD entiende que aún se están debatiendo disposiciones específicas sobre la protección de los datos personales. El CEPD sigue estando disponible para más contribuciones y pide una participación temprana y más proactiva de las autoridades de protección de datos en la preparación de estas disposiciones específicas, a fin de garantizar una comprensión y consideración óptimas de las salvaguardias de protección de datos.

Proyecto provisional de disposiciones sobre equipos conjuntos de investigación e investigaciones conjuntas (ECI) (artículo 3), sobre la solicitud de información de registro de nombres de dominio (artículo 6) y sobre la revelación rápida de los datos informáticos almacenados en caso de emergencia (artículo 7).

Sobre la base de su evaluación preliminar, el CEPD recomienda seguir examinando el proyecto de disposiciones provisional en relación con los siguientes elementos.

El CEPD observa que tanto las solicitudes de información sobre el registro de nombres de dominio como de revelación rápida de datos informáticos almacenados en casos de emergencia son solicitudes no vinculantes y los motivos de denegación de la solicitud no están claramente definidos, mientras que tampoco está clara la posibilidad de basarse en la legislación del Estado Parte requerido para

[11] Véanse los asuntos acumulados C-402/05 P y C-415/05 P del TJUE, Kadi/Consejo, ECLI:EU:C:2008:461, apartado 285.

denegar dicha cooperación, incluidos los motivos de denegación establecidos en los tratados de asistencia judicial mutua[12]. A este respecto, el CEPD recuerda que las condiciones en las que los proveedores de servicios de comunicaciones electrónicas o la entidad que presta servicios de nombres de dominio deben conceder dicho acceso deben estar previstas en la ley, a fin de garantizar que el tratamiento se apoye en una base jurídica clara.

El CEPD se remite además a su contribución anterior para restablecer que, excepto en casos de urgencia legítimamente establecida[13] y, a la luz de la jurisprudencia del TJUE[14], el CEPD considera que el tipo de autoridades solicitantes que pueden emitir dicha solicitud debe limitarse a un fiscal, una autoridad judicial u otra autoridad independiente. El CEPD considera también que la participación sistemática de las autoridades judiciales en las partes requeridas es esencial para garantizar un examen del cumplimiento efectivo de las solicitudes de conformidad con el Convenio y para preservar la aplicación del principio de doble tipificación en el ámbito de la cooperación judicial.

A este respecto, el CEPD recuerda que el principio de doble tipificación tiene por objeto proporcionar una salvaguardia adicional para garantizar que una Parte no pueda contar con la asistencia otra para aplicar una sanción penal, que no existe en la legislación de esta otra Parte. Además de garantizar el respeto de los derechos de las personas y las garantías procesales en el mecanismo previsto de cooperación judicial, dicha salvaguardia también proporciona una garantía esencial relacionada con las condiciones procesales para el acceso a sus datos personales. Como ya se mencionó en su contribución anterior, en relación con la seguridad del tratamiento de datos, el CEPD invita al T-CY a considerar, como salvaguardia específica de la protección de datos, un mecanismo para la notificación sin demora de las violaciones de datos que puedan interferir gravemente con los derechos y libertades de los interesados. En efecto, las violaciones de datos personales podrían tener una serie de efectos adversos significativos para los individuos afectados.

En relación con el proyecto provisional de disposiciones sobre la solicitud de información relativa al registro de nombres de dominio, el CEPD subraya que dicha información incluye datos personales y que, por lo tanto, todo instrumento internacional que establezca condiciones de fondo y forma para acceder a dichos datos, para los miembros Parte de la Unión Europea, debe cumplir con el Derecho primario y derivado de la UE.

En relación con el proyecto provisional de disposiciones sobre la «revelación rápida de datos informáticos almacenados en caso de emergencia» (artículo 7), el CEPD señala que, dependiendo de su aplicación por cada Parte, esta nueva disposición puede implicar la revelación directa de datos de contenido. El CEPD también señala que el Estado parte requerido puede exigir, tras la revelación de los datos, que se facilite una solicitud de asistencia mutua adecuada (artículo 7, apartado 5). Sin embargo, en este último caso, las Partes en el Protocolo previsto no se comprometen a suprimir los datos o a no utilizarlos como prueba si, sobre la base de la información complementaria obtenida en la solicitud de asistencia mutua adecuada, las autoridades requeridas concluyen que no se cumplían las condiciones para revelar los datos. Por lo tanto, las consecuencias jurídicas respecto de los datos revelados, una vez en el país solicitante, parecen dejarse completamente a la discreción de la legislación nacional de ese país. La falta de compromiso al nivel del protocolo entraña, por tanto, el

[12] El proyecto de artículo 6, apartado 2, se remite, por ejemplo, a las «condiciones razonables previstas por el Derecho interno».

[13] El CEPD señala que el concepto de emergencia se menciona en el sentido del apartado 1 del proyecto de disposición relativa a los procedimientos de urgencia para las solicitudes de asistencia jurídica mutua y considera que el alcance de esta situación puede aclararse y enmarcarse con mayor precisión.

[14] Véanse los asuntos acumulados C-203/15 P y C-698/15 P del TJUE, Tele2 Sverige AB, ECLI:EU:C:2016:970, apartado 120.

riesgo de privar a esta disposición de cualquier efecto protector en lo que respecta al tratamiento de los datos personales ya revelados.

Por último, el CEPD subraya el requisito establecido en el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la UE[15], según el cual cualquier limitación al ejercicio de los derechos y libertades reconocidos por la Carta está sujeta al principio de proporcionalidad y solo podrá introducirse si es necesario. Por lo tanto, para ser lícito con arreglo al Derecho de la UE, el proyecto de disposiciones del Protocolo previsto debe cumplir este requisito. A continuación, se refiere tanto a los datos personales contenidos en la solicitud como a la respuesta a dicha solicitud. **Por lo tanto, al CEPD le preocupa especialmente la redacción del proyecto de artículo 6, apartado 3, letra c), y del proyecto de informe explicativo, apartado 13, en relación con esta disposición, lo que parece implicar que los terceros países solicitantes que son parte en el Protocolo previsto pueden no estar obligados a respetar el principio de proporcionalidad al enviar solicitudes a un Estado miembro de la UE**. Además, no está totalmente clara la posibilidad que ofrecen estas disposiciones de invocar el principio de proporcionalidad como motivo de denegación.

Tampoco está claro si las Partes estarían obligadas a garantizar, en el contexto del Protocolo previsto, las condiciones y salvaguardias establecidas en el artículo 15 del Convenio de Budapest[16]. **El CEPD recomienda aclarar que las obligaciones establecidas en el artículo 15 del Convenio de Budapest se aplican plenamente también en el contexto de esta cooperación transfronteriza.**

Disposiciones sobre las garantías de protección de datos

El CEPD considera esencial que el texto provisional hecho público se complemente con disposiciones específicas sobre garantías de protección de datos, que luego deben evaluarse junto con otras disposiciones, a fin de garantizar que el proyecto de Protocolo adicional se traduzca en un acuerdo sostenible para el intercambio de datos personales con terceros países con fines coercitivos, plenamente compatible con los Tratados de la UE y la Carta de los Derechos Fundamentales.

El proyecto provisional de disposiciones sobre la solicitud de información para el registro de nombres de dominio y la revelación rápida de los datos informáticos almacenados en caso de emergencia, mediante el establecimiento de condiciones de procedimiento para el acceso a los datos personales, puede ya repercutir en el nivel de protección de los datos personales y también puede ser necesario modificarlo para garantizar la aplicación operativa de las garantías adecuadas en materia de protección de datos. **A este respecto, el CEPD desea señalar una vez más la necesidad de que las salvaguardias de protección de datos se apliquen a todo intercambio de datos personales en el contexto del Protocolo previsto[17], incluso en relación con la transferencia de datos personales[18].**

El CEPD considera que las disposiciones específicas sobre las garantías de protección de datos deben reflejar principios fundamentales, en particular la legalidad, la equidad y la transparencia, la limitación de la finalidad, la minimización de datos, la exactitud, la limitación del almacenamiento, la integridad y la confidencialidad. Del mismo modo, el CEPD desea subrayar la importancia de garantizar los derechos individuales fundamentales (acceso, rectificación y supresión), de limitar cualquier restricción mediante el principio de proporcionalidad, y de ejercer una tutela judicial efectiva para los interesados en caso de violación de las salvaguardias de protección de datos. El ejercicio de estos derechos también requiere notificación al interesado, al menos una vez que ya no se ponga en peligro

[15] Véase también el artículo 8, apartado 2, del Convenio Europeo de Derechos Humanos.
[16] Véase, en particular, el artículo 6, apartado 4.
[17] El artículo 6, apartado 4, parece limitar la aplicación de las salvaguardias, así como del artículo 15 del Convenio, a la información revelada exclusivamente, y no a los datos personales incluidos en la solicitud.
[18] De acuerdo con el proyecto de informe explicativo, apartado 9, esta última disposición solo puede/debe aplicarse a la transferencia de datos personales en virtud de los equipos conjuntos de investigación.

la investigación. Estos principios, derechos y obligaciones también están en consonancia con la versión modernizada del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos de carácter personal (Convenio 108 +), del que también son Partes muchas Partes en el Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el Convenio 108 +, deben aplicarse a todas las autoridades que traten los datos en la Parte solicitante, a fin de garantizar la continuidad de la protección. **El CEPD se remite a su contribución en la consulta pública de 2019 para más detalles sobre los requisitos de la UE a este respecto**[19].

El CEPD reitera la importancia de implicar a las autoridades de protección de datos en el proceso de elaboración del Protocolo adicional y está dispuesto a contribuir y ayudar al T-CY a preparar el texto provisional de las disposiciones sobre garantías de protección de datos.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf