Consejo de la Unión Europea

Bruselas, 2 de diciembre de 2021
(OR. en)

14614/21

Expediente interinstitucional: 2021/0383(NLE)

JAI 1333
COPEN 433
CYBER 321
ENFOPOL 483
TELECOM 453
EJUSTICE 106
MI 913
DATAPROTECT 277

PROPUESTA

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	25 de noviembre de 2021
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2021) 719 final
Asunto:	Propuesta de DECISIÓN DEL CONSEJO por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas

Adjunto se remite a las Delegaciones el documento – COM(2021) 719 final.

Adj.: COM(2021) 719 final

COMISIÓN
EUROPEA

Bruselas, 25.11.2021
COM(2021) 719 final

2021/0383 (NLE)

Propuesta de

DECISIÓN DEL CONSEJO

por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas

EXPOSICIÓN DE MOTIVOS

1. OBJETO DE LA PROPUESTA

La presente propuesta se refiere a la Decisión por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), relativo a la cooperación reforzada y la revelación de pruebas electrónicas («el Protocolo»)[1]. El objetivo del Protocolo es establecer reglas internacionales comunes para reforzar la cooperación en materia de ciberdelincuencia y de obtención de pruebas en formato electrónico en las investigaciones y los procesos penales.

La presente propuesta complementa la propuesta paralela de la Comisión de Decisión del Consejo de la Unión Europea («el Consejo») por la que se autoriza a los Estados miembros a firmar el Protocolo en interés de la Unión Europea.

La ciberdelincuencia sigue representando un gran problema para nuestra sociedad. A pesar de la labor que desempeñan las autoridades policiales y judiciales, los ciberataques y, especialmente, los ataques con programas de secuestro están aumentando y son cada vez más complejos[2]. En particular, el carácter transfronterizo de internet hace que las investigaciones en materia de ciberdelincuencia se extiendan a más de un territorio estatal, lo que requiere una cooperación estrecha entre las autoridades de distintos países.

Las pruebas electrónicas son cada vez más importantes en las investigaciones penales. La Comisión estima que, actualmente, las autoridades policiales y judiciales necesitan pruebas electrónicas en el 85 % de las investigaciones penales, sobre todo en el caso de la ciberdelincuencia[3]. Cada vez es más frecuente que las pruebas de los delitos las conserven en formato electrónico proveedores de servicios en otros países, y para que la justicia penal actué con eficacia son precisas medidas adecuadas que permitan obtener dichas pruebas a fin de defender el Estado de Derecho.

En todo el mundo se está tratando de mejorar la disponibilidad transfronteriza de las pruebas electrónicas para las investigaciones penales: a nivel nacional, a nivel de la Unión Europea[4] y en foros internacionales, especialmente a través del Protocolo. Es importante garantizar la compatibilidad de las normas en el plano internacional para así evitar conflictos de leyes cuando se soliciten pruebas electrónicas.

2. CONTEXTO DE LA PROPUESTA

2.1. Antecedentes

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest del Consejo de Europa (STCE n.º 185) («el Convenio») tiene por objeto facilitar la lucha contra los delitos que se sirven de las redes informáticas. Este 1) contiene disposiciones que armonizan los elementos sustantivos de los tipos penales y las disposiciones conexas en el ámbito de la ciberdelincuencia, 2) dispone las competencias procesales nacionales necesarias para la

[1] El texto del Protocolo se adjunta como anexo de la presente propuesta.
[2] Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea de 2021 (SOCTA, por sus siglas en inglés).
[3] SWD(2018) 118 final.
[4] COM(2018) 225 y 226 final.

investigación y el enjuiciamiento de tales delitos, así como de otros delitos cometidos mediante un sistema informático o cuando las pruebas estén en formato electrónico, y 3) tiene por objeto establecer un régimen rápido y eficaz de cooperación internacional.

El Convenio está abierto a los Estados miembros del Consejo de Europa y a quienes no sean miembros previa invitación. En la actualidad, 66 países son partes en el Convenio, incluidos 26 Estados miembros de la Unión Europea[5]. El Convenio no contempla que la Unión Europea pueda adherirse al Convenio. No obstante, la Unión Europea está reconocida como organización observadora del Comité del Convenio sobre la Ciberdelincuencia («el Comité del Convenio»)[6].

A pesar del intento de negociar un nuevo convenio sobre ciberdelincuencia a nivel de las Naciones Unidas[7], el Convenio de Budapest sigue siendo el principal convenio multilateral de la lucha contra la ciberdelincuencia. El apoyo de la Unión al Convenio es férreo[8]; por ejemplo, en el marco de la financiación de programas de desarrollo de capacidades[9].

A raíz de las propuestas del Grupo sobre pruebas en la nube[10], el Comité del Convenio adoptó varias recomendaciones para tratar, especialmente mediante la negociación del Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación internacional reforzada, la dificultad de que cada vez más las pruebas electrónicas en materia de ciberdelincuencia y otros delitos obran en poder de proveedores de servicios en otros países, mientras que las competencias de las autoridades policiales siguen estando limitadas por las fronteras territoriales. En junio de 2017, el Comité del Convenio aprobó el mandato para la preparación del Protocolo adicional segundo durante el período comprendido entre septiembre de 2017 y diciembre de 2019[11]. Habida cuenta de la necesidad de disponer de más tiempo para concluir los debates, así como de las limitaciones planteadas por la pandemia de COVID-19 en 2020 y 2021, el Comité del Convenio prorrogó posteriormente el mandato dos veces, primero hasta diciembre de 2020 y luego hasta mayo de 2021.

A raíz del llamamiento del Consejo Europeo en sus Conclusiones de 18 de octubre de 2018[12], la Comisión adoptó el 5 de febrero de 2019 una Recomendación de Decisión del Consejo por la que se autoriza la participación en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia[13]. El Supervisor Europeo de

---

5 Todos excepto Irlanda, que ha firmado pero no ratificado el Convenio, si bien se ha comprometido a proseguir el proceso de adhesión.

6 Reglamento interno del Comité del Convenio sobre la Ciberdelincuencia [T-CY (2013) 25 rev], que se puede consultar en: www.coe.int/cybercrime.

7 Resolución 74/247 de la Asamblea General de las Naciones Unidas, de 27 diciembre de 2019, «Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos».

8 JOIN(2020) 81 final.

9 Véase, por ejemplo, la Acción Mundial Ampliada contra la Ciberdelincuencia ampliada (GLACY+), en https://www.coe.int/en/web/cybercrime/glacyplus.

10 Informe final del Grupo sobre pruebas en la nube (Cloud Evidence Group) del Comité del Convenio: «Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY» (Acceso de la justicia penal a las pruebas electrónicas en la nube: recomendaciones para su examen por el Comité del Convenio) de 16 de septiembre de 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690.

12 https://www.consilium.europa.eu/es/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

Protección de Datos aprobó un dictamen sobre la Recomendación el 2 de abril de 2019[14]. Mediante Decisión de 6 de junio de 2019, el Consejo de la Unión Europea autorizó a la Comisión a participar, en nombre de la Unión Europea, en las negociaciones del Protocolo adicional segundo[15].

Tal como se expresa en la Estrategia de la UE para una Unión de la Seguridad, de 2020[16], la Estrategia de Ciberseguridad de la UE para la Década Digital, de 2020[17], y la Estrategia de la UE contra la Delincuencia Organizada, de 2021[18], la Comisión se ha comprometido a llevar las negociaciones del Protocolo a buen puerto con rapidez. El Parlamento Europeo también reconoció la necesidad de concluir los trabajos preparativos del Protocolo en su Resolución de 2021 sobre la Estrategia de Ciberseguridad de la UE para la Década Digital[19].

La Comisión participó, en nombre de la Unión Europea, en las negociaciones del Protocolo de conformidad con la Decisión del Consejo de la Unión Europea. La Comisión consultó sistemáticamente al comité especial del Consejo para las negociaciones sobre la posición de la Unión.

En consonancia con el Acuerdo marco sobre las relaciones entre el Parlamento Europeo y la Comisión Europea[20], la Comisión también informó al Parlamento Europeo de las negociaciones mediante informes escritos y presentaciones orales.

En la sesión plenaria del Comité del Convenio de 28 de mayo de 2021, el Comité dio su aprobación al proyecto de Protocolo y lo remitió para su adopción por el Comité de Ministros del Consejo de Europa[21]. El 17 de noviembre de 2021, el Comité de Ministros del Consejo de Europa adoptó el Protocolo.

2.2. El Protocolo adicional segundo

El objetivo del Protocolo es reforzar la cooperación en materia de ciberdelincuencia y de obtención de pruebas en formato electrónico de delitos a efectos de investigaciones y procesos penales específicos. El Protocolo reconoce la necesidad de una cooperación mayor y más eficiente entre los Estados y con el sector privado, así como la necesidad que tienen los proveedores de servicios y demás entidades de una claridad y seguridad jurídica mayores en relación con las circunstancias en las que pueden atender las solicitudes de las autoridades penales de otros Estados Parte de revelación de pruebas electrónicas.

El Protocolo también reconoce que, para que la cooperación transfronteriza en materia penal sea eficaz, especialmente entre las autoridades del sector público y las entidades del sector privado, son precisas unas condiciones eficaces y unas salvaguardias sólidas para la protección de los derechos fundamentales. A tal fin, el Protocolo articula un planteamiento anclado en los derechos y establece condiciones y salvaguardias en consonancia con los

[14] Dictamen 3/2019 del SEPD, de 2 abril de 2019, relativo a la participación en las negociaciones del Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia (Convenio de Budapest).
[15] Decisión del Consejo 9116/19.
[16] COM(2020) 605 final.
[17] JOIN(2020) 81 final.
[18] COM(2021) 170 final.
[19] Resolución del Parlamento Europeo, de 10 de junio de 2021, sobre la Estrategia de Ciberseguridad de la UE para la Década Digital.
[20] Referencia L 304/47.
[21] https://rm.coe.int/0900001680a2aa42.

instrumentos internacionales de derechos humanos, como el Convenio del Consejo de Europa para la protección de los derechos humanos y de las libertades fundamentales, de 1950. Dado que las pruebas electrónicas contienen a menudo datos personales, el Protocolo también incluye salvaguardias sólidas para la protección de la privacidad y los datos personales.

Las disposiciones mencionadas en los párrafos siguientes revisten especial importancia dentro del Protocolo. El Protocolo va acompañado de un Informe explicativo pormenorizado. Aunque el Informe explicativo no constituye un instrumento que dé una interpretación autorizada del Protocolo, su objetivo es «orientar y asistir a las Partes» en la aplicación del Protocolo[22].

2.2.1. Disposiciones comunes

El capítulo I del Protocolo establece las disposiciones comunes. El artículo 2 determina el ámbito de aplicación del Protocolo, en consonancia con el ámbito de aplicación del Convenio: se aplica a investigaciones o procesos penales específicos relativos a delitos relacionados con datos y sistemas informáticos, y a la obtención de pruebas en formato electrónico de delitos.

El artículo 3 define los términos «autoridad central», «autoridad competente», «emergencia», «datos personales» y «Parte transmitente». Estas definiciones, junto con las definiciones del Convenio, rigen en todo el Protocolo.

El artículo 4 determina los idiomas en que las Partes deben enviar los requerimientos, solicitudes y notificaciones contemplados en el Protocolo.

2.2.2. Medidas de cooperación

El capítulo II del Protocolo dispone medidas para reforzar la cooperación. En primer lugar, el artículo 5, apartado 1, establece que las Partes cooperarán en el marco del Protocolo en la mayor medida posible. El artículo 5, apartados 2 a 5, determina la aplicación de las medidas del Protocolo en relación con los tratados o acuerdos de asistencia mutua en vigor. El artículo 5, apartado 7, establece que las medidas del capítulo II no restringirán la cooperación entre las Partes, o con proveedores de servicios o entidades, que contemplen otros convenios, acuerdos, prácticas o normas de Derecho interno aplicables.

El artículo 6 sienta las bases para la cooperación directa entre las autoridades competentes de una Parte y las entidades que prestan servicios de registro de nombres de dominio en el territorio de otra Parte a efectos de la revelación de datos de registro de nombres de dominio.

El artículo 7 sienta las bases para la cooperación directa entre las autoridades competentes de una Parte y los proveedores de servicios de otra Parte a efectos de la revelación de datos de abonados.

El artículo 8 sienta las bases para la cooperación reforzada entre autoridades a efectos de la revelación de datos informáticos.

El artículo 9 sienta las bases para la cooperación entre autoridades a efectos de la revelación de datos informáticos en situaciones de emergencia.

El artículo 10 sienta las bases para la asistencia judicial mutua en situaciones de emergencia.

---

[22] Véase el apartado 2 del Informe explicativo del Protocolo.

El artículo 11 sienta las bases para la cooperación por videoconferencia.

El artículo 12 sienta las bases para las investigaciones conjuntas y los equipos conjuntos de investigación.

2.2.3. Salvaguardias

El Protocolo articula un planteamiento anclado en los derechos que incorpora condiciones y salvaguardias específicas, algunas de las cuales se incluyen en las medidas específicas de cooperación, así como en el capítulo III del Protocolo. El artículo 13 del Protocolo exige a las Partes que se cercioren de que en el ejercicio de las competencias y en los procedimientos se brinde un nivel adecuado de protección de los derechos fundamentales, lo que, de conformidad con el artículo 15 del Convenio, garantiza la aplicación del principio de proporcionalidad.

El artículo 14 del Protocolo dispone la protección de los datos personales, tal como se definen en el artículo 3 del Protocolo en consonancia con el Derecho de la Unión y con el Protocolo modificativo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 223) (Convenio 108+).

Partiendo de esta base, el artículo 14, apartados 2 a 15, establece principios fundamentales de protección de datos, como la limitación de la finalidad, la base jurídica, la calidad de los datos y las reglas aplicables al tratamiento de categorías especiales de datos, obligaciones aplicables a los responsables del tratamiento, especialmente en materia de conservación, llevanza de registros, seguridad y en lo que respecta a las transferencias ulteriores, derechos individuales exigibles, especialmente en materia de notificación, acceso, rectificación y toma de decisiones automatizadas, supervisión independiente y eficaz por parte de una o más autoridades, así como vías de resarcimiento administrativas y judiciales. Las salvaguardias abarcan todas las formas de cooperación establecidas en el Protocolo, con las adaptaciones que sean necesarias para ajustarse a las características específicas de la cooperación directa en cuestión (por ejemplo, en el contexto de la notificación de infracciones). El ejercicio de determinados derechos individuales puede retrasarse, limitarse o denegarse cuando sea necesario y proporcionado para perseguir objetivos importantes de interés público y, en particular, no poner en riesgo las investigaciones policiales en curso, lo que también está en consonancia con el Derecho de la Unión.

El artículo 14 del Protocolo debe leerse en relación con el artículo 23 del Protocolo. El artículo 23 refuerza la eficacia de las salvaguardias del Protocolo al disponer que el Comité del Convenio sobre la Ciberdelincuencia evaluará la ejecución y aplicación de las medidas adoptadas en la legislación nacional para dar efecto a las disposiciones del Protocolo. En particular, el artículo 23, apartado 3, reconoce explícitamente que la aplicación del artículo 14 por las Partes se evaluará una vez que diez Partes en el Convenio hayan manifestado su consentimiento para obligarse por el Protocolo.

Otro ejemplo de salvaguardia, recogida en el artículo 14, apartado 15, es que, cuando una Parte tenga pruebas sustanciales de que otra Parte incumple de forma sistemática o grave las salvaguardias establecidas en el Protocolo, puede suspender la transferencia de datos personales a dicha Parte previa consulta (lo cual no es necesario en caso de urgencia). Los datos personales transferidos antes de la suspensión se seguirán tratando de conformidad con el Protocolo.

Por último y habida cuenta del carácter multilateral del Protocolo, el artículo 14, apartado 1, letras b) y c), del Protocolo permite a las Partes acordar en sus relaciones bilaterales, en determinadas condiciones, formas alternativas de garantizar la protección de los datos personales transferidos en virtud del Protocolo. Si bien las salvaguardias del artículo 14, apartados 2 a 15, se aplican por defecto a las Partes que reciben datos personales en virtud del artículo 14, apartado 1, letra b), las Partes vinculadas entre sí por un acuerdo internacional que establezca un marco global de protección de los datos personales en consonancia con los requisitos aplicables de la legislación de las Partes en cuestión también pueden basarse en dicho marco. Es el caso, por ejemplo, del Convenio 108+ (respecto de las Partes que permiten que se realicen transferencias de datos a otras Partes en virtud de dicho Convenio) o del Acuerdo marco UE-EE. UU. (dentro de su ámbito de aplicación, es decir, respecto de la transferencia de datos personales entre autoridades y, en combinación con un acuerdo específico de transferencia entre los Estados Unidos y la UE, respecto de la cooperación directa entre autoridades y proveedores de servicios). Además, basándose en el artículo 14, apartado 1, letra c), las Partes también pueden determinar con carácter mutuo que la transferencia de datos personales tenga lugar basándose en otros acuerdos o convenios entre las Partes en cuestión. En el caso de los Estados miembros de la UE, este acuerdo o convenio alternativo solo puede invocarse respecto de las transferencias de datos realizadas en virtud del Protocolo si dichas transferencias cumplen los requisitos de la normativa de la Unión en materia de protección de datos, a saber, el capítulo V de la Directiva (UE) 2016/680 (Directiva sobre protección de datos en el ámbito penal) y, respecto de la cooperación directa entre autoridades y proveedores de servicios contemplada en los artículos 6 y 7 del Protocolo, el capítulo V del Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

2.2.4. Disposiciones finales

El capítulo IV del Protocolo establece las disposiciones finales. Una de las cosas que garantiza el artículo 15, apartado 1, letra a), es que las Partes puedan regular de modo distinto sus relaciones respecto de las cuestiones contempladas en el Protocolo, en consonancia con el artículo 39, apartado 2, del Convenio. El artículo 15, apartado 1, letra b), garantiza que los Estados miembros de la UE que sean Partes en el Protocolo puedan seguir aplicando el Derecho de la Unión en sus relaciones recíprocas. El artículo 15, apartado 2, determina asimismo que el artículo 39, apartado 3, del Convenio es de aplicación al Protocolo.

El artículo 16, apartado 3, indica que el Protocolo no entrará en vigor hasta que cinco Partes en el Convenio hayan manifestado su consentimiento para obligarse por el Protocolo.

El artículo 19, apartado 1, establece que las Partes pueden formular reservas en relación con el artículo 7, apartado 9, letras a) y b), el artículo 8, apartado 13, y el artículo 17. El artículo 19, apartado 2, establece que las Partes pueden realizar declaraciones en relación con el artículo 7, apartado 2, letra b), y apartado 8, el artículo 8, apartado 11, el artículo 9, apartado 1, letra b), y apartado 5, el artículo 10, apartado 9, el artículo 12, apartado 3, y el artículo 18, apartado 2. El artículo 19, apartado 3, dispone que las Partes pueden realizar las declaraciones, notificaciones o comunicaciones contempladas en el artículo 7, apartado 5, letras a) y e), el artículo 8, apartado 4 y apartado 10, letras a) y b), el artículo 14, apartado 7, letra c), y apartado 10, letra b), y el artículo 17, apartado 2.

El artículo 23, apartado 1, sienta las bases para las consultas entre las Partes, especialmente a través del Comité del Convenio, de conformidad con el artículo 46 del Convenio. El artículo 23, apartado 2, también sienta las bases para valorar el uso y la aplicación de las disposiciones del Protocolo. El artículo 23, apartado 3, garantiza que la valoración del uso y la aplicación del artículo 14, relativo a la protección de datos, no comience hasta que diez Partes hayan manifestado su consentimiento para obligarse por el Protocolo.

2.3. Derecho y política de la Unión en este ámbito

El ámbito regulado por el Protocolo está cubierto en gran medida por normas comunes basadas en el artículo 82, apartado 1, y el artículo 16 del TFUE. El marco jurídico actual de la Unión Europea se compone, en particular, de instrumentos sobre cooperación policial y judicial en materia penal, como la Directiva 2014/41/UE, relativa a la orden europea de investigación en materia penal, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea y la Decisión Marco 2002/465/JAI del Consejo, sobre equipos conjuntos de investigación. En la dimensión exterior, la Unión Europea ha celebrado una serie de acuerdos bilaterales entre la Unión y terceros países, como los acuerdos de asistencia judicial entre la Unión Europea y los Estados Unidos de América, entre la Unión Europea y Japón y entre la Unión Europea y Noruega e Islandia. También se integra en el marco jurídico actual de la Unión Europea el Reglamento (UE) 2017/1939 del Consejo, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea. Los Estados miembros que participen en la cooperación reforzada deben velar por que la Fiscalía Europea pueda, en el ejercicio de las competencias que le otorgan los artículos 22, 23 y 25 del Reglamento (UE) 2017/1939, recurrir a la cooperación contemplada en el Protocolo del mismo modo que los fiscales nacionales de dichos Estados miembros. Estos instrumentos y acuerdos se refieren, en particular, a los artículos 8, 9, 10, 11 y 12 del Protocolo.

Además, la Unión ha adoptado varias directivas que refuerzan los derechos procesales de los investigados y encausados[23]. Estos instrumentos se refieren, en particular, a los artículos 6, 7, 8, 9, 10, 11, 12 y 13 del Protocolo. Un conjunto particular de salvaguardias se refiere a la protección de los datos personales, que es un derecho fundamental consagrado en los Tratados de la UE y en la Carta de los Derechos Fundamentales de la Unión Europea. Los datos personales solo pueden tratarse de conformidad con el Reglamento (UE) 2016/679 (el Reglamento general de protección de datos) y la Directiva (UE) 2016/680 (Directiva sobre protección de datos en el ámbito penal). El derecho fundamental de toda persona al respeto de su vida privada y familiar, su domicilio y sus comunicaciones incluye el respeto del secreto de las comunicaciones como un elemento esencial. Los datos de las comunicaciones electrónicas solo pueden tratarse de conformidad con la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas). Estos instrumentos se refieren, en particular, al artículo 14 del Protocolo.

[23] Directiva 2010/64/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, relativa al derecho a interpretación y a traducción en los procesos penales (DO L 280 de 26.10.2010, p. 1); Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales (DO L 142 de 1.6.2012, p. 1); Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad (DO L 294 de 6.11.2013, p. 1); Directiva (UE) 2016/1919 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, relativa a la asistencia jurídica gratuita a los sospechosos y acusados en los procesos penales y a las personas buscadas en virtud de un procedimiento de orden europea de detención (DO L 297 de 4.11.2016, p. 1); Directiva (UE) 2016/800 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales (DO L 132 de 21.5.2016, p. 1); Directiva (UE) 2016/343 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio (DO L 65 de 11.3.2016, p. 1); y Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales.

El artículo 14, apartados 2 a 15, del Protocolo establece salvaguardias adecuadas de protección de datos en el sentido de la normativa de protección de datos de la Unión y, en particular, el artículo 46 del Reglamento general de protección de datos y el artículo 37 de la Directiva sobre protección de datos en el ámbito penal, así como la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea. En consonancia con los requisitos del Derecho de la Unión[24] y con el fin de garantizar la eficacia de las salvaguardias establecidas en el artículo 14 del Protocolo, los Estados miembros deben garantizar la notificación de las personas cuyos datos se hayan transferido, con sujeción a determinadas restricciones, por ejemplo, para no poner en riesgo las investigaciones en curso. El artículo 14, apartado 11, letra c), del Protocolo sienta las bases para que los Estados miembros cumplan este requisito.

La compatibilidad del artículo 14, apartado 1, del Protocolo con la normativa de protección de datos de la Unión también exige que los Estados miembros consideren lo siguiente con respecto a las posibles formas alternativas de garantizar una protección adecuada de los datos personales transferidos en virtud del Protocolo. Por lo que se refiere a otros acuerdos internacionales que establezcan un marco global de protección de los datos personales en consonancia con los requisitos aplicables de la legislación de las Partes en cuestión, en virtud del artículo 14, apartado 1, letra b), los Estados miembros deben tener en cuenta que, a efectos de la cooperación directa, el Acuerdo marco UE-EE. UU. debe complementarse con salvaguardias adicionales, que se establecerán en un acuerdo específico de transferencia entre los Estados Unidos y la UE o sus Estados miembros, que tengan en cuenta la especificidad de los requisitos para la transferencia de pruebas electrónicas directamente por los proveedores de servicios y no entre autoridades[25].

Asimismo, de conformidad con el artículo 14, apartado 1, letra b), del Protocolo, los Estados miembros deben considerar que, para los Estados miembros de la UE que son Partes en el Convenio 108+, dicho Convenio no constituye por sí mismo una base adecuada para las transferencias transfronterizas de datos realizadas en virtud del Protocolo a otras Partes en dicho Convenio. A este respecto, deben tener en cuenta la última frase del artículo 14, apartado 1, del Convenio 108+[26].

---

[24] Véase el dictamen 1/15 del Tribunal de Justicia (Gran Sala), ECLI:EU:C:2017:592, apartado 220. Véase también la contribución del CEPD a la consulta sobre el proyecto de Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), de 13 de noviembre de 2019, p. 6 («Las autoridades nacionales competentes a las que se ha concedido acceso a los datos deben notificar a las personas afectadas, con arreglo a los procedimientos nacionales aplicables, tan pronto como dicha notificación ya no pueda poner en peligro las investigaciones emprendidas por dichas autoridades. [...] La notificación es necesaria para que las personas afectadas puedan ejercer su derecho a la tutela judicial efectiva y sus derechos de protección de datos en relación con el tratamiento de sus datos»).

[25] Esta es la razón por la que la Decisión del Consejo, de 21 de mayo de 2019, por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal (9114/19), contiene en sus directrices de negociación una serie de salvaguardias en materia de protección de datos. En particular, las directrices de negociación establecen que «[e]l Acuerdo debe complementar el Acuerdo Marco con garantías adicionales que tengan en cuenta el nivel de sensibilidad de las categorías de datos afectadas y la especificidad de los requisitos para la transferencia de pruebas electrónicas directamente por los proveedores de servicios en lugar de entre autoridades y las transferencias de las autoridades competentes directas a los proveedores de servicios».

[26] Véase también el Informe explicativo del Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 10 de octubre de 2018, puntos 106 y 107.

Por último, por lo que respecta a los otros acuerdos o convenios contemplados en el artículo 14, apartado 1, letra c), los Estados miembros deben considerar que solo pueden basarse en esos otros acuerdos o convenios, bien si la Comisión Europea ha adoptado una decisión de adecuación de conformidad con el artículo 45 del Reglamento general de protección de datos[(UE) 2016/679] o el artículo 36 de la Directiva sobre protección de datos en el ámbito penal [(UE) 2016/680] en relación con el tercer país en cuestión que abarque las transferencias de datos correspondientes, bien si ese otro acuerdo o convenio establece salvaguardias adecuadas de protección de datos con arreglo al artículo 46 del Reglamento general de protección de datos o al artículo 37, apartado 1, letra a), de la Directiva sobre protección de datos en el ámbito penal.

No solo debe tenerse en cuenta el Derecho de la Unión en su estado actual en el ámbito de que se trate, sino también su evolución futura, en la medida en que sea previsible en el momento del análisis. El ámbito regulado por el Protocolo es directamente pertinente para la evolución previsible del Derecho de la Unión en el futuro. A este respecto, procede hacer mención a las propuestas de la Comisión sobre el acceso transfronterizo a las pruebas electrónicas, de abril de 2018[27]. Estos instrumentos se refieren, en particular, a los artículos 6 y 7 del Protocolo.

La Comisión, al tiempo que participaba en las negociaciones en nombre de la Unión, se aseguró de que el Protocolo fuera plenamente compatible con el Derecho de la Unión y con las obligaciones de los Estados miembros derivadas de este. En particular, la Comisión garantizó que las disposiciones del Protocolo permitiesen a los Estados miembros respetar los derechos fundamentales, las libertades y los principios generales del Derecho de la Unión consagrados en los Tratados de la UE y en la Carta de los Derechos Fundamentales de la Unión Europea, especialmente la proporcionalidad, los derechos procesales, la presunción de inocencia y los derechos de defensa de las personas incursas en procesos penales, así como la privacidad y la protección de los datos personales y de las comunicaciones electrónicas cuando se traten dichos datos y, en particular, en las transferencias a las autoridades policiales en países no pertenecientes a la Unión Europea, así como cualquier obligación que incumba a las autoridades policiales y judiciales a este respecto. La Comisión también tuvo en cuenta el dictamen del Supervisor Europeo de Protección de Datos[28] y del Comité Europeo de Protección de Datos[29].

Además, la Comisión se aseguró de que las disposiciones del Protocolo y las propuestas de la Comisión en materia de pruebas electrónicas fueran compatibles, sobre todo a medida que las iniciativas legislativas evolucionaban en los debates con los colegisladores, y el Protocolo no dé lugar a conflictos de leyes. En particular, la Comisión garantizó que el Protocolo incluyera salvaguardias adecuadas en materia de protección de datos y privacidad, lo que permite a los proveedores de servicios de la UE cumplir las obligaciones que le impone la normativa de la UE en materia de protección de datos y privacidad, dado que el Protocolo establece una base

[27] COM(2018) 225 y 226 final.

[28] Dictamen 3/2019 del SEPD, de 2 abril de 2019, relativo a la participación en las negociaciones del Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia (Convenio de Budapest).

[29] Véanse: la contribución del CEPD a la consulta sobre el proyecto de Segundo protocolo adicional al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), de 13 de noviembre de 2019; la Declaración 02/2021, sobre el nuevo proyecto de disposiciones del protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), en su versión adoptada el 2 de febrero de 2021; la contribución del CEPD a la sexta ronda de consultas sobre el proyecto de Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), de 4 de mayo de 2021.

jurídica para las transferencias de datos con motivo de los requerimientos o solicitudes de una autoridad de una Parte en el Protocolo que no pertenezca a la UE que exijan a un responsable o encargado del tratamiento de la UE revelar datos personales o datos de comunicaciones electrónicas.

2.4. Reservas, declaraciones, notificaciones y comunicaciones, y otras consideraciones

El Protocolo sienta las bases para que las Partes puedan formular determinadas reservas y realizar declaraciones, notificaciones o comunicaciones en relación con determinados artículos. Los Estados miembros deben asumir un planteamiento uniforme con respecto a determinadas reservas y las declaraciones, notificaciones y comunicaciones que figuran en el anexo de la presente Decisión. Para garantizar la compatibilidad de la aplicación del Protocolo con el Derecho de la Unión, los Estados miembros de la UE deben adoptar la posición que figura a continuación con respecto a dichas reservas y declaraciones. Cuando el Protocolo sirva de base para otras reservas, declaraciones, notificaciones o comunicaciones, la presente propuesta autoriza a los Estados miembros a realizar sus propias reservas, declaraciones, notificaciones o comunicaciones si lo consideran conveniente.

A fin de garantizar la compatibilidad entre las disposiciones del Protocolo y el Derecho y las políticas pertinentes de la Unión, los Estados miembros no deben formular las reservas contempladas en el artículo 7, apartado 9, letras a)[30] y b)[31]. Además, los Estados miembros deben realizar la declaración contemplada en el artículo 7, apartado 2, letra b)[32], y la notificación contemplada en el artículo 7, apartado 5, letra a)[33]. La ausencia de estas reservas y la presentación de la declaración y la notificación son importantes para garantizar la compatibilidad del Protocolo con las iniciativas legislativas de la Comisión en materia de pruebas electrónicas, sobre todo a medida que las iniciativas legislativas evolucionen en los debates con los colegisladores.

Además, a fin de garantizar una aplicación uniforme del Protocolo por parte de los Estados miembros de la UE al cooperar con Partes que no sean Estados miembros de la UE, se anima a los Estados miembros a no formular una reserva con arreglo al artículo 8, apartado 13[34], porque tal reserva produciría efectos recíprocos[35]. Los Estados miembros deben realizar la declaración contemplada en el artículo 8, apartado 4, para garantizar que pueda darse efecto a los requerimientos en caso de que se necesite información justificativa adicional, como, por

---

[30] Permite a las Partes reservarse el derecho a inaplicar el artículo 7 (revelación de datos de abonados).

[31] Permite a las Partes reservarse el derecho a inaplicar el artículo 7 (revelación de datos de abonados) respecto de determinados tipos de números de acceso si ello es contrario a los principios fundamentales de su ordenamiento jurídico interno.

[32] Permite a las Partes declarar que el requerimiento del artículo 7, apartado 1 (revelación de datos de abonados), debe ser dictado por un fiscal u otra autoridad judicial, o estar bajo su supervisión, o ser dictado bajo supervisión independiente.

[33] Permite a las Partes notificar a la Secretaría General del Consejo de Europa que, cuando se dicta un requerimiento con arreglo al artículo 7, apartado 1 (revelación de datos de abonados) cuyo destinatario sea un proveedor de servicios que se encuentre en su territorio, la Parte exige, en todos los casos o en circunstancias determinadas, la notificación simultánea del requerimiento, de la información suplementaria y de un resumen de los hechos relacionados con la investigación o el proceso.

[34] Permite a las Partes reservarse el derecho a inaplicar el artículo 8 (dar efecto a los requerimientos de otra Parte) respecto de los datos relativos al tráfico.

[35] Véase el apartado 147 del Informe explicativo del Protocolo, que dice que una Parte que formule reserva con arreglo a este artículo no está autorizada a enviar requerimientos de datos relativos al tráfico a otras Partes con arreglo al artículo 8, apartado 1.

ejemplo, sobre las circunstancias del caso de que se trate, a fin de valorar la proporcionalidad y la necesidad[36].

También se anima a los Estados miembros a no realizar la declaración contemplada en el artículo 9, apartado 1, letra b)[37], a fin de garantizar una aplicación eficiente del Protocolo.

Los Estados miembros deben efectuar las comunicaciones contempladas en el artículo 7, apartado 5, letra e)[38], el artículo 8, apartado 10, letras a) y b)[39], el artículo 14, apartado 7, letra c), y apartado 10, letra b), para garantizar una aplicación general eficaz del Protocolo[40].

Por último, los Estados miembros también deben tomar las medidas necesarias de conformidad con el artículo 14, apartado 11, letra c), para garantizar que la Parte receptora sea informada, en el momento de la transferencia, de la obligación que impone el Derecho de la Unión de notificar a la persona a la que se refieren los datos[41], así como que se le comuniquen datos de contacto adecuados para que dicha Parte receptora pueda informar a la autoridad competente del Estado miembro de la UE una vez que ya no se apliquen las restricciones de confidencialidad y se pueda proceder a la notificación.

2.5. Motivación de la propuesta

El Protocolo no entrará en vigor hasta que cinco Partes hayan manifestado su consentimiento para obligarse por el Protocolo de conformidad con lo dispuesto en el artículo 16, apartados 1 y 2. Está previsto que la ceremonia de firma del Protocolo se celebre en marzo de 2022.

Los Estados miembros de la UE deben tomar las medidas necesarias para garantizar que el Protocolo se ratifique y entre en vigor rápidamente, aspecto este que reviste importancia por una serie de factores.

En primer lugar, el Protocolo garantizará que las autoridades policiales y judiciales disponen de medios mejores para obtener las pruebas electrónicas necesarias para las investigaciones penales. Vista la importancia creciente de las pruebas electrónicas para las investigaciones penales, es perentorio que las autoridades policiales y judiciales dispongan de los instrumentos adecuados para tener acceso a las pruebas electrónicas de manera que puedan luchar eficazmente contra la delincuencia en línea.

En segundo lugar, el Protocolo garantizará que tales medidas para tener acceso a las pruebas electrónicas permitan que los Estados miembros puedan respetar los derechos fundamentales,

---

[36] Permite a las Partes declarar que es precisa información justificativa adicional para dar efecto a los requerimientos contemplados en el artículo 8, apartado 1 (dar efecto a los requerimientos de otra Parte).

[37] Permite a las Partes que declaren que no ejecutarán las solicitudes contempladas en el artículo 9, apartado 1, letra a) (revelación rápida de datos informáticos en caso de emergencia) que pretendan únicamente la revelación de datos de abonados.

[38] Permite a las Partes comunicar los datos de contacto de la autoridad que designen para recibir notificaciones con arreglo al artículo 7, apartado 5, letra a), y llevar a cabo las actuaciones descritas en el artículo 7, apartado 5, letras b), c) y d) (revelación de datos de abonados).

[39] Permite a las Partes comunicar la información de contacto de las autoridades designadas para cursar y recibir los requerimientos contemplados en el artículo 8 (dar efecto a los requerimientos de otra Parte). De conformidad con los requisitos del Reglamento (UE) 2017/1939, los Estados miembros que participen en la cooperación reforzada para la creación de la Fiscalía Europea incluirán a esta en la comunicación.

[40] Permite a las Partes comunicar la autoridad o autoridades a las que se debe, respectivamente, notificar en caso de incidente que afecte a la seguridad o contactar para solicitar autorización previa en caso de transferencias ulteriores a otro Estado u organización internacional.

[41] Véase la nota a pie de página 24.

especialmente los derechos procesales penales, el derecho a la privacidad y el derecho a la protección de los datos personales. A falta de normas claras de escala internacional, las prácticas existentes pueden plantear dificultades desde el punto de vista de la seguridad jurídica, la transparencia, la rendición de cuentas y el respeto de los derechos fundamentales y las garantías procesales de los investigados.

En tercer lugar, el Protocolo resolverá y evitará conflictos de leyes que afecten tanto a las autoridades como a los proveedores de servicios del sector privado y a otras entidades, estableciendo reglas internacionales compatibles para el acceso transfronterizo a las pruebas electrónicas.

En cuarto lugar, el Protocolo demostrará la importancia que sigue teniendo el Convenio como principal marco multilateral para la lucha contra la ciberdelincuencia. Este aspecto tendrá una importancia crítica en el proceso posterior a la Resolución 74/247 de la Asamblea General de las Naciones Unidas, de 27 diciembre de 2019, «Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos», que estableció un comité intergubernamental especial de expertos de composición abierta a fin de elaborar un convenio internacional integral sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos.

3. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- *Base jurídica*

La competencia de la Unión para legislar en asuntos relativos a la facilitación de la cooperación entre autoridades judiciales o equivalentes en relación con los procesos penales y la ejecución de resoluciones se basa en el artículo 82, apartado 1, del TFUE. La competencia de la Unión en materia de protección de datos personales se basa en el artículo 16 del TFUE.

Conforme al artículo 3, apartado 2, del TFUE, la Unión tiene competencia exclusiva para la celebración de un acuerdo internacional en la medida en que dicha celebración pueda afectar a normas comunes de la UE o alterar el alcance de las mismas. Las disposiciones del Protocolo entran en un ámbito cubierto en gran medida por normas comunes, como se indica en la sección 2.3.

Por lo tanto, el Protocolo es competencia externa exclusiva de la Unión. Así pues, la ratificación del Protocolo por parte de los Estados miembros, en interés de la Unión, puede llevarse a cabo sobre la base del artículo 16, el artículo 82, apartado 1, y el artículo 218, apartado 6, del TFUE.

- *Subsidiariedad (en el caso de competencia no exclusiva)*

No procede.

- *Proporcionalidad*

Los objetivos de la Unión en relación con la presente propuesta, tal como se exponen en la sección 2.5, solo pueden lograrse mediante la celebración de un acuerdo internacional vinculante que disponga las medidas de cooperación necesarias, garantizando al mismo tiempo una protección adecuada de los derechos fundamentales. El Protocolo logra este objetivo. Las disposiciones del Protocolo se limitan a lo necesario para alcanzar sus objetivos principales. La acción unilateral no constituye una verdadera alternativa, ya que no proporcionaría una base suficiente para la cooperación con países no pertenecientes a la UE y no podría garantizar la necesaria protección de los derechos fundamentales. Asimismo, la

adhesión a un acuerdo multilateral como el Protocolo, que la Unión ha podido negociar, es más eficiente que entablar negociaciones bilaterales con países no pertenecientes a la UE. En el supuesto de que las 66 Partes, así como las futuras nuevas Partes en el Convenio, ratifiquen el Protocolo, este constituirá un marco jurídico común para la cooperación de los Estados miembros de la UE con sus socios internacionales más importantes en la lucha contra la delincuencia.

- ***Elección del instrumento***

No procede.

4. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- *Evaluaciones* ex post */ controles de la adecuación de la legislación existente*

No procede.

- *Consultas con las partes interesadas*

El Consejo de Europa organizó seis rondas de consultas públicas en relación con las negociaciones del Protocolo, en julio y noviembre de 2018, febrero y noviembre de 2019, diciembre de 2020 y mayo de 2021[42]. Las partes examinaron las aportaciones recibidas en el marco de estas consultas.

La Comisión, como negociadora en nombre de la Unión, también intercambió pareceres con las autoridades de protección de datos y organizó reuniones de consulta específicas a lo largo de 2019 y 2021 con organizaciones de la sociedad civil, proveedores de servicios y asociaciones comerciales. La Comisión tuvo en cuenta las aportaciones recibidas en estos intercambios.

- *Obtención y uso de asesoramiento especializado*

En el proceso de negociación, la Comisión consultó sistemáticamente al comité especial del Consejo para las negociaciones, de conformidad con la Decisión del Consejo de la Unión Europea, de 6 de junio de 2019, por la que se autoriza a la Comisión a participar en las negociaciones en nombre de la Unión, lo que brindó a los expertos de los Estados miembros la oportunidad de contribuir al proceso de formulación de la posición de la Unión. Varios expertos de los Estados miembros también siguieron participando en las negociaciones junto a la Comisión, que actuaba en nombre de la Unión. También se celebraron consultas con las partes interesadas (véase más arriba).

- *Evaluación de impacto*

En 2017-2018 se llevó a cabo una evaluación de impacto que acompañara a las propuestas de la Comisión en materia de pruebas electrónicas[43]. En este contexto, la negociación de un acuerdo sobre el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia (Convenio de Budapest) formaba parte de la opción preferida. Además, en la presente exposición de motivos se exponen los efectos pertinentes.

---

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations.

[43] SWD(2018) 118 final.

- *Adecuación regulatoria y simplificación*

El Protocolo puede tener implicaciones para determinadas categorías de proveedores de servicios, especialmente las pymes, ya que pueden ser objeto de solicitudes y requerimientos de pruebas electrónicas en virtud del Protocolo. Sin embargo, en la actualidad, estos proveedores a menudo ya están sujetos a tales solicitudes a través de otros instrumentos existentes, a veces transmitidas a través de distintas autoridades, en particular sobre la base del Convenio[44], otros tratados de asistencia judicial mutua u otros marcos aplicables, como las políticas multilaterales de gobernanza de internet[45]. Asimismo, los proveedores de servicios y, en particular, las pymes, saldrán beneficiadas con un marco jurídico internacional claro y un planteamiento común de todas las Partes en el Protocolo.

- *Derechos fundamentales*

Es probable que los instrumentos de cooperación contemplados en el Protocolo afecten a los derechos fundamentales cuando los datos de una persona puedan obtenerse en el contexto de un proceso penal y, en particular, al derecho a un juez imparcial, el derecho a la privacidad y el derecho a la protección de los datos personales. El Protocolo articula un planteamiento anclado en los derechos y establece condiciones y salvaguardias en consonancia con los instrumentos internacionales de derechos humanos, como el Convenio del Consejo de Europa para la protección de los derechos humanos y de las libertades fundamentales, de 1950. En particular, el Protocolo establece salvaguardias específicas en materia de protección de datos. De ser necesario, el Protocolo también faculta a las Partes para que formulen determinadas reservas y realicen ciertas declaraciones o notificaciones e incluye motivos para no cooperar en situaciones específicas. De este modo se garantiza la compatibilidad del Protocolo con la Carta de los Derechos Fundamentales de la UE.

5. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene repercusiones presupuestarias para el presupuesto de la Unión. Es posible que los Estados miembros deban sufragar gastos puntuales para aplicar el Protocolo; el coste para las autoridades de los Estados miembros podría ser mayor debido al aumento previsto del número de casos.

6. OTROS ELEMENTOS

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

No existe ningún plan de ejecución, ya que, tras su firma y ratificación, los Estados miembros estarán obligados a aplicar el Protocolo.

Por lo que se refiere al seguimiento, la Comisión participará en las reuniones del Comité del Convenio, en las que se reconoce a la Unión Europea como organización observadora.

---

[44] Véase, por ejemplo, la Nota Orientativa n.º 10 del Comité del Convenio, de 1 de marzo de 2017, sobre las órdenes de presentación de información relativa a abonados (artículo 18 del Convenio de Budapest).

[45] Véase, por ejemplo, la Resolución de la Junta de la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés), de 15 de mayo de 2019, sobre las recomendaciones relativas a la especificación temporal para datos de registro gTLD (las siglas «gTLD» se refieren a los denominados «dominios genéricos de primer nivel»), que se puede consultar en www.icann.org.

2021/0383 (NLE)

Propuesta de

DECISIÓN DEL CONSEJO

por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16, su artículo 82, apartado 1, y su artículo 218, apartado 6,

Vista la propuesta de la Comisión Europea,

Vista la aprobación del Parlamento Europeo,

Considerando lo siguiente:

(1) El 9 de junio de 2019, el Consejo autorizó a la Comisión a participar, en nombre de la Unión, en las negociaciones sobre el Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest).

(2) El texto del Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas (en lo sucesivo, «el Protocolo»), fue adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021 y está previsto que se abra a la firma en marzo de 2022.

(3) Las disposiciones del Protocolo pertenecen a un ámbito regulado en gran medida por normas comunes en el sentido del artículo 3, apartado 2, del TFUE, incluidos los instrumentos que facilitan la cooperación judicial en materia penal y garantizan normas mínimas para los derechos procesales, así como salvaguardias en materia de protección de datos y privacidad.

(4) La Comisión también presentó una propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal [COM(2018) 225 final] 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 [COM(2018) 226 final], con las que se introducían órdenes europeas de entrega y conservación transfronterizas vinculantes que deben dirigirse directamente a un representante de un proveedor de servicios en otro Estado miembro.

(5) Con su participación en las negociaciones en nombre de la Unión, la Comisión veló por la compatibilidad del Protocolo adicional segundo con las normas comunes pertinentes de la Unión Europea.

(6) Por medio de una serie de reservas, declaraciones, notificaciones y comunicaciones se puede garantizar la compatibilidad del Protocolo con el Derecho y las políticas de la Unión, así como la aplicación uniforme del Protocolo por los Estados miembros de la

UE en sus relaciones con Partes no pertenecientes a la UE, y la aplicación efectiva del Protocolo.

(7) Dado que el Protocolo establece procedimientos rápidos que mejoran el acceso transfronterizo a las pruebas electrónicas y salvaguardias de alto nivel, la entrada en vigor contribuirá a la lucha contra la ciberdelincuencia y otras formas de delincuencia de escala mundial, facilitando la cooperación entre los Estados miembros de la UE y los Estados no miembros de la UE que sean Partes en el Protocolo, otorgará un nivel elevado de protección a las personas y tratará la cuestión de los conflictos de leyes.

(8) Dado que el Protocolo establece salvaguardias adecuadas en consonancia con los requisitos que imponen a las transferencias internacionales de datos personales el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, su entrada en vigor contribuirá a promover las normas de protección de datos de la Unión en todo el mundo, facilitará los flujos de datos entre los Estados miembros de la UE y los Estados no miembros de la UE que sean Partes en el Protocolo y garantizará el cumplimiento por parte de los Estados miembros de la UE de las obligaciones que les atribuyen las normas de protección de datos de la Unión.

(9) La rápida entrada en vigor del Protocolo confirmará además la importancia del Convenio de Budapest del Consejo de Europa como principal marco multilateral para la lucha contra la ciberdelincuencia.

(10) La Unión Europea no puede convertirse en Parte en el Protocolo, ya que tanto el Protocolo como el Convenio del Consejo de Europa sobre la Ciberdelincuencia solo están abiertos a la firma de los Estados.

(11) Por lo tanto, debe autorizarse a los Estados miembros a ratificar el Protocolo, actuando conjuntamente en interés de la Unión Europea.

(12) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, emitió su dictamen el ….

(13) [De conformidad con los artículos 1 y 2 del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda no participa en la adopción de la presente Decisión y no queda vinculada por ella ni sujeta a su aplicación.]

[O]

[De conformidad con los artículos 1 y 2 del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda ha notificado [, por carta de ... ,] su deseo de participar en la adopción y aplicación de la presente Decisión.]

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

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Los Estados miembros quedan autorizados a ratificar, en interés de la Unión Europea, el Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas («el Protocolo»).

Artículo 2

Al ratificar el Protocolo, los Estados miembros realizarán las reservas, declaraciones, notificaciones o comunicaciones que figuran en el anexo.

Artículo 3

La presente Decisión entrará en vigor el día de su adopción.

Artículo 4

La presente Decisión se publicará en el Diario Oficial de la Unión Europea.

Artículo 5

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el

Por el Consejo
El Presidente / La Presidenta