Comisión Europea

CONVOCATORIA DE DATOS PARA UNA EVALUACIÓN DE IMPACTO

TÍTULO DE LA INICIATIVA	Evaluación de impacto sobre la conservación de datos por parte de los proveedores de servicios en los procesos penales
DG PRINCIPAL (UNIDAD RESPONSABLE)	HOME.D4
TIPO PROBABLE DE INICIATIVA	
CALENDARIO ORIENTATIVO	Primer trimestre de 2026
INFORMACIÓN COMPLEMENTARIA	Ciberdelincuencia – Comisión Europea; Grupo de Alto Nivel sobre el acceso a los datos para la aplicación eficaz de la ley – Comisión Europea

A. Contexto político, definición del problema y control de la subsidiariedad

Contexto político

Para poder combatir y enjuiciar eficazmente los delitos, cabe la posibilidad de que las autoridades policiales y judiciales necesiten acceder a determinados datos sin contenido tratados por los proveedores de servicios de comunicaciones electrónicas. A falta de obligaciones específicas que exijan que dichos proveedores conserven los datos durante un período de tiempo razonable y limitado, puede ocurrir que, para cuando las autoridades los soliciten en el contexto de procesos penales, los datos ya se hayan suprimido. En la actualidad, no existe un marco jurídico a escala de la UE en este ámbito. En el seno de la UE, las legislaciones nacionales de que dispone la mayoría de los Estados miembros son divergentes, mientras que otros Estados miembros no cuentan con normas al respecto. La policía, la fiscalía y las autoridades judiciales determinaron que la ausencia de normas armonizadas de conservación de datos para las categorías fundamentales de datos constituía un reto importante para los procesos penales a escala nacional de los delitos que se producen tanto en línea como fuera de línea, reto que obstaculiza la cooperación transfronteriza en toda la UE. El tema se consideró de suma importancia en el Grupo de Alto Nivel sobre el acceso a los datos, en el que los expertos recomendaron la adopción de un marco de la UE sobre la conservación de datos a efectos de la aplicación de la ley que incluyera también garantías de acceso. Recientemente, la presidenta de la Comisión, Úrsula von der Leyen, (1) (2) y los Estados miembros de la UE, en las Conclusiones del Consejo sobre el acceso a los datos para una aplicación eficaz de la ley y sobre el refuerzo de las iniciativas antiterroristas conjuntas, subrayaron la necesidad de adoptar medidas para garantizar un acceso lícito y efectivo a los datos a efectos de aplicación de la ley. En la Comunicación ProtectEU: una Estrategia Europea para la Seguridad Interior, la Comisión se comprometió a presentar en 2025 una hoja de ruta en la que se expusiese el camino a seguir en relación con el acceso legal y efectivo a los datos por parte de los servicios policiales y a dar prioridad a una evaluación del impacto de las normas de conservación de datos a escala de la UE.

Problema que la iniciativa se propone afrontar

En una sociedad digital, las pruebas electrónicas son fundamentales en la mayoría de las investigaciones y los enjuiciamientos penales. Los datos sin contenido (como la información del abonado, la fuente y el destino de un mensaje, la ubicación del dispositivo, la fecha, la hora, la duración, el tamaño u otro tipo de interacción que no incluya el contenido de las comunicaciones) podrían ser decisivos para identificar o localizar a sospechosos o acusados y víctimas, y para arrojar luz en general sobre la comisión de un delito. Los proveedores de servicios de comunicaciones electrónicas

almacenan los datos sin contenido de las comunicaciones que pasan por sus sistemas. Dado que estos datos sin contenido pueden ser de carácter personal y proporcionar información sobre la vida privada de las personas a las que se refieren, de conformidad con los derechos fundamentales (en particular los artículos 7, 8 y 11 de la Carta) y la legislación de la UE en materia de privacidad y protección de datos, los proveedores de servicios deben suprimirlos cuando dejen de ser necesarios para fines comerciales legítimos. El almacenamiento de datos durante períodos de tiempo más prolongados solo es posible si existen obligaciones jurídicas específicas que así lo exijan. A raíz de la decisión del Tribunal de Justicia de la Unión Europea de declarar inválida la Directiva de la UE sobre la conservación de datos a causa de una injerencia grave en los derechos fundamentales y de la falta de garantías específicas de acceso, desde 2014, el Derecho de la UE ya no impone a los proveedores de servicios la obligación de conservar datos a efectos de aplicación de la ley. Si bien estas obligaciones existen en muchos Estados miembros de la UE, existen discrepancias sustanciales entre sus legislaciones en lo que respecta a los requisitos que regulan la conservación. Como consecuencia de ello, la policía y los fiscales se enfrentan a obstáculos a la hora de hacer su trabajo, ya que a menudo los datos necesarios no están disponibles o han dejado de estarlo para cuando se lleva a cabo la investigación. En la situación actual, algunos delitos, en particular los que se producen exclusivamente en línea, no pueden investigarse y enjuiciarse de manera eficiente.

Los proveedores de servicios de comunicaciones electrónicas también se enfrentan a costes y obstáculos más elevados a la hora de ofrecer sus servicios en la UE, debido a que tienen que cumplir diferentes requisitos jurídicos en los distintos Estados miembros y como consecuencia de los frecuentes cambios en las legislaciones nacionales a raíz de sentencias a escala nacional o de la UE[1]. Además, la mayoría de las leyes nacionales sobre conservación de datos solo se aplican a las plataformas de telecomunicaciones tradicionales, y no contemplan a los proveedores de comunicaciones que ofrecen sus servicios a través de internet, que actualmente son los servicios de comunicación más utilizados. Las discrepancias existentes entre las legislaciones nacionales también afectan a los ciudadanos, dado que para cuando se llevan a cabo las investigaciones penales ya se han eliminado los datos sin contenido necesarios. En ese caso, es posible que las autoridades no puedan ser capaces de impartir justicia y proteger adecuadamente a los ciudadanos. Es probable que estas divergencias entre las legislaciones nacionales sigan aumentando con la aparición de las nuevas tecnologías y servicios de comunicación digital que se desarrollen en el futuro.

La situación actual puede obedecer a la falta de requisitos y garantías armonizados para que los proveedores de servicios de comunicaciones electrónicas, basados o no en la numeración, conserven los datos más allá del tiempo requerido para sus necesidades comerciales específicas, de manera que los datos puedan seguir estando disponibles durante más tiempo a efectos de aplicación de la ley.

Base para la actuación de la UE (base jurídica y control de subsidiariedad)

Base jurídica

[1] El reciente análisis de Eurojust y la Red Judicial Europea sobre Ciberdelincuencia (RJEC) «*The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*» (El efecto de la jurisprudencia del Tribunal de Justicia de la Unión Europea en los regímenes nacionales de conservación de datos y la cooperación judicial en la UE) indica que doce Estados miembros (BE, DK, EE, IE, FR, HR, IT, LV, LT, PT, SK y SE) introdujeron importantes cambios en su legislación entre 2018 y 2022 a raíz del asunto C-746/18 del TJUE, Prokuratuur, y de los asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, y que cuatro Estados miembros ya no cuentan con normas obligatorias de conservación de datos a efectos de investigaciones penales (DE, NL, RO, SI), p. 6.

La base jurídica debe decidirse y depende del resultado de la evaluación de impacto.

Necesidad práctica de la actuación de la UE

Los retos identificados no pueden ser abordados satisfactoriamente por los Estados miembros por sí solos. A falta de una actuación a escala de la UE, se espera que los Estados miembros sigan actualizando su legislación nacional para aplicar los requisitos de la jurisprudencia del Tribunal de Justicia de la UE, del Tribunal Europeo de Derechos Humanos y de los órganos jurisdiccionales nacionales. También tendrán que dar respuesta a las tecnologías nuevas y emergentes, lo que entraña el riesgo de que las discrepancias entre las normas sean cada vez mayores. Esto agravará los efectos negativos en los ciudadanos, las investigaciones penales, los proveedores de servicios de comunicaciones electrónicas y otras partes interesadas pertinentes de la UE. Al mismo tiempo, es necesario garantizar que la injerencia de las obligaciones de conservación de datos y acceso en los derechos fundamentales de los usuarios sea proporcionada, tal como se establece en la jurisprudencia del Tribunal de Justicia de la Unión Europea. Las leyes sobre conservación de datos inciden en diversos ámbitos políticos, como la seguridad, la justicia, los derechos fundamentales y la economía, y afectan a diferentes partes interesadas (por ejemplo, autoridades, empresas y ciudadanos). Habida cuenta del impacto en el mercado interior de la UE y en el espacio de libertad, seguridad y justicia de la UE, la actuación a escala de la UE para abordar los problemas detectados podría considerarse la manera más adecuada de avanzar. El principal objetivo de la actuación de la UE podría ser garantizar la aplicación armonizada de las obligaciones de conservación de datos para los proveedores de servicios, incluidas garantías sobre el acceso de las autoridades policiales y judiciales, a fin de velar por la seguridad jurídica de las partes interesadas pertinentes y la igualdad de condiciones para los proveedores de servicios que ofrecen sus servicios dentro de la UE.

B. Objetivos y opciones de actuación

El objetivo general de la iniciativa es garantizar la disponibilidad de determinadas categorías de datos sin contenido con el fin de poder llevar a cabo investigaciones y enjuiciamientos penales, respetando y salvaguardando al mismo tiempo las normas de la UE para la protección de los derechos fundamentales, y preservando la ciberseguridad y la integridad del mercado de la UE.

Para lograrlo, la Comisión estudiará y evaluará diferentes opciones, entre las que se incluyen las siguientes:

- medidas de Derecho indicativo para mejorar la cooperación entre las autoridades públicas y los proveedores de servicios de comunicaciones electrónicas, basados o no en la numeración, como normas comunes a escala de la UE para la categorización de datos, formularios para solicitar y facilitar datos, directrices sobre los períodos mínimos de conservación de los datos de los abonados y las direcciones IP con sello de tiempo, y cooperación voluntaria;
- medidas legislativas que establezcan requisitos obligatorios para todos los proveedores de servicios contemplados por el Código Europeo de las Comunicaciones Electrónicas[2] para la conservación de datos sin contenido y el acceso a los mismos, de conformidad con la jurisprudencia existente del Tribunal de Justicia de la Unión Europea. Podrían concebirse diferentes soluciones legislativas en función de los datos sin contenido que deban conservarse y del delito que se persiga.

La opción más adecuada se determinará durante la evaluación de impacto, sobre la base de las pruebas recogidas y la consulta a las partes interesadas, y tras comparar las diferentes opciones.

[2] Artículo 2, apartado 4, de la Directiva (UE) 2018/1972: «servicio de comunicaciones electrónicas»: el prestado por lo general a cambio de una remuneración a través de redes de comunicaciones electrónicas, que incluye, con la excepción de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos, los siguientes tipos de servicios:

a) el «servicio de acceso a internet», entendido según la definición del punto 2) del párrafo segundo del artículo 2 del Reglamento (UE) 2015/2120;

b) el «servicio de comunicaciones interpersonales», y

c) servicios consistentes, en su totalidad o principalmente, en el transporte de señales, como son los servicios de transmisión utilizados para la prestación de servicios máquina a máquina y para la radiodifusión.

C. Repercusiones probables

Se espera que esta iniciativa tenga repercusiones positivas en varios ámbitos:

Repercusiones sociales: la disponibilidad de datos sin contenido ayudaría a las autoridades públicas a detectar, investigar y enjuiciar los delitos con mayor eficacia, garantizando así una sociedad más segura, tanto en línea como fuera de línea, para los ciudadanos de la UE. Se espera que las repercusiones positivas afecten tanto a los procesos penales nacionales como a la cooperación transfronteriza para luchar contra la delincuencia.

Repercusiones económicas: los proveedores de servicios de comunicaciones electrónicas evitarán los costes adicionales de cumplimiento y la inseguridad jurídica resultantes de los diferentes requisitos jurídicos y técnicos en función del Estado o Estados miembros de la UE en los que estén establecidos o en los que operen. La iniciativa evaluará las formas de reducir los obstáculos a la provisión de servicios en el mercado interior de la UE. Al mismo tiempo, la iniciativa hará que aumenten los costes de conservación de datos en los Estados miembros en los que no exista la obligación de conservación de datos a efectos de aplicación de la ley.

Repercusiones en los derechos fundamentales: los datos sin contenido conservados y consultados podrían proporcionar a las autoridades información sobre la vida privada de las personas a las que se refieren estos datos e interferir, por tanto, en los derechos fundamentales que protegen su privacidad (artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea), sus datos personales (artículo 8) y su libertad de expresión (artículo 11). La mejora de la capacidad de las autoridades públicas para recuperar datos sin contenido y obtener pruebas en procesos penales serviría al interés público de una detección y enjuiciamiento más eficaces de los delitos y a la libertad de prestar servicios en el mercado interior de la UE, y podría traducirse en más justicia para las víctimas, los sospechosos y los acusados. Cuando las opciones consideradas en la evaluación de impacto limiten los derechos fundamentales, se ponderarán con la interferencia en dichos derechos, y se tendrá plenamente en cuenta la posibilidad de ofrecer garantías adecuadas para velar por su necesidad y proporcionalidad para alcanzar el objetivo perseguido.

D. Instrumentos de mejora de la legislación

Evaluación de impacto

La Comisión efectuará una evaluación de impacto con el fin de actualizar las normas sobre conservación de datos a escala de la UE, según proceda. En el segundo o el tercer trimestre de 2025 se publicará una consulta pública con arreglo a la política de mejora de la legislación de la Comisión. La Comisión llevará a cabo una recopilación exhaustiva de pruebas procedentes de diferentes fuentes, incluido el público a través de diferentes medios, como la presente convocatoria pública de datos, y encuestas dirigidas a las partes interesadas pertinentes.

Estrategia de consulta

La Comisión prevé varias actividades de consulta para apoyar esta iniciativa. Su objetivo es recabar pruebas y opiniones de una amplia gama de partes interesadas. Las principales actividades de consulta incluirán:

- observaciones sobre esta convocatoria de datos;
- comentarios sobre una consulta pública que se publicará en todas las lenguas oficiales de la UE en el sitio web de la Comisión «Díganos lo que piensa» durante un período de doce semanas;
- consultas específicas a las partes interesadas pertinentes en forma de entrevistas y encuestas para recopilar también pruebas cuantitativas y cualitativas sobre la necesidad y proporcionalidad de estas medidas.

En consonancia con la política de mejora de la legislación de la Comisión, que fomenta el desarrollo de iniciativas basadas en los mejores conocimientos disponibles, también se invita a los investigadores científicos, a las organizaciones académicas y a las sociedades y asociaciones científicas con

experiencia en los ámbitos técnicos y políticos relacionados con la iniciativa, a que presenten investigaciones, análisis y datos científicos pertinentes, tanto publicados como en ediciones preliminares. La Comisión está especialmente interesada en las observaciones que sinteticen el estado actual de los conocimientos en los ámbitos pertinentes.

La Comisión publicará un informe de síntesis fáctico con las contribuciones a la consulta pública. Asimismo, analizará los comentarios a la presente convocatoria de datos y los resultados de las consultas posteriores en un informe de síntesis adjunto a la evaluación de impacto (documento de trabajo de los servicios de la Comisión).

¿Por qué se realiza la consulta?

El objetivo de la consulta es garantizar que la evaluación de impacto se base en amplios conocimientos y datos cuantitativos y cualitativos, y permitir a las partes interesadas (incluidos los ciudadanos y las personas que se verían directamente afectadas por esta iniciativa) presentar sus puntos de vista y sus aportaciones sobre las posibles opciones para el camino a seguir.

Público destinatario

Entre las principales categorías de partes interesadas que la Comisión tiene previsto consultar figuran las siguientes: el público en general; los profesionales que operan en los sectores de la seguridad pública (justicia, asuntos de interior y políticas digitales); las autoridades policiales y judiciales; los expertos en ciberseguridad y las autoridades de protección de datos y privacidad; las asociaciones de abogados profesionales, el mundo académico, los investigadores y los grupos de reflexión; las organizaciones de la sociedad civil que trabajan en la defensa de las víctimas de violaciones de los derechos digitales o, más en general, de los derechos fundamentales, y las empresas del sector.