Consejo de la Unión Europea

Bruselas, 3 de octubre de 2025
(OR. en)

13029/25

COPEN 272
CYBER 252
ENFOPOL 330
JAI 1275
DATAPROTECT 222
COSI 163
IXIM 199
CATS 46
FREMP 241
TELECOM 310
CT 117

NOTA

De:	Secretaría General del Consejo
A:	Comité de Representantes Permanentes/Consejo
Asunto:	Acceso a los datos para una investigación penal eficaz - Estado de los trabajos

Garantizar el acceso lícito a los datos sobre comunicaciones electrónicas a los efectos de la aplicación de la ley y de las investigaciones penales es un asunto prioritario para el Consejo y resulta especialmente necesario en el contexto de la lucha contra el terrorismo y la delincuencia grave y organizada.

En consonancia con la labor del Grupo de Alto Nivel sobre el Acceso a los Datos para una Aplicación Eficaz de la Ley (en lo sucesivo, el «Grupo de Alto Nivel»), que emitió recomendaciones[1] en mayo de 2024 y un informe final[2] en noviembre de 2024, y a fin de dar cumplimiento a las Conclusiones del Consejo sobre el acceso a los datos para una aplicación eficaz de la ley[3] de 12 de diciembre de 2024, la Comisión presentó una Hoja de ruta para un acceso lícito y efectivo a los datos por parte de las autoridades policiales y judiciales[4] el 24 de junio de 2025 (en lo sucesivo, la «hoja de ruta»). En sus Conclusiones de 26 de junio de 2025, el Consejo Europeo invitó a las instituciones de la UE y a los Estados miembros a que refuercen la cooperación policial y la judicial, incluido el acceso efectivo a datos con fines policiales[5].

En particular, la Presidencia desea llamar la atención de los ministros de Justicia sobre las cuestiones de la conservación de datos (1), la interceptación legal de comunicaciones (2) y el desafío horizontal del cifrado (3).

1. La conservación de datos

«Conservación de datos» hace referencia a la obligación impuesta a los proveedores de servicios de conservar datos sin contenido (información relativa a los abonados, direcciones IP, metadatos de tráfico y de localización) durante un período determinado para que puedan ponerse a disposición de las autoridades policiales con fines de investigación penal.

El Grupo de Alto Nivel dedicó uno de los tres capítulos de su informe final a la conservación de datos. Entre las dificultades más importantes, el informe hace hincapié en la actual fragmentación de la legislación nacional y en los desafíos adicionales que presentan los proveedores de servicios de transmisión libre («over-the-top» u OTT), incluidas las aplicaciones de mensajería para teléfonos móviles que se utilizan de manera generalizada. Como posible solución, el Grupo de Alto Nivel propuso crear normas mínimas armonizadas para el acceso a los datos y su conservación. También abogó por reforzar la cooperación entre los proveedores de datos y los profesionales.

1 11281/24.
2 15941/2/24 REV2.
3 16448/24.
4 10806/25.
5 EUCO 12/25.

En su hoja de ruta, la Comisión indicó su intención de preparar una evaluación de impacto con vistas a actualizar, según proceda, las normas de la UE sobre conservación de datos. La evaluación de impacto se puso en marcha en mayo de 2025 y se espera que finalice en el primer trimestre de 2026. Asimismo, la Comisión instó a Europol y Eurojust a seguir trabajando para racionalizar la cooperación con los proveedores de servicios de comunicaciones y a desarrollar, en colaboración con esos proveedores, un catálogo de los datos que estos procesan para sus fines profesionales.

En el Consejo, el Grupo «Cooperación Judicial en Materia Penal» (Grupo «COPEN») dedicó su reunión del 19 de mayo de 2025 a la cuestión de la conservación de datos, centrándose en una posible propuesta legislativa de la UE sobre este asunto. El 25 de septiembre de 2025 se celebró una segunda reunión, en la que el Grupo «COPEN» debatió el contenido y los criterios que serían adecuados para ese instrumento, también a la luz de los requisitos establecidos en la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE). En ambos casos, el objetivo era cambiar impresiones y contribuir a los trabajos que la Comisión está llevando a cabo.

La Presidencia considera que, dependiendo del resultado de la evaluación de impacto de la Comisión, un avance clave en 2026 podría ser la apertura de un debate sobre una propuesta legislativa para regular la conservación de datos en la UE.

2. La interceptación legal de comunicaciones

La interceptación legal de comunicaciones permite a las autoridades obtener acceso encubierto a las comunicaciones en tiempo real[6].

En su informe final, el Grupo de Alto Nivel señaló que «[s]i bien la interceptación legal de telecomunicaciones tradicionales sigue siendo una herramienta fundamental en muchas investigaciones, la eficacia de esta medida ha disminuido drásticamente dado que, actualmente, la mayoría de los servicios de telecomunicaciones son prestados por otros actores: según diversas fuentes, cerca del 97 % de todos los mensajes móviles se envía ahora mediante aplicaciones de mensajería como WhatsApp, Facebook Messenger y WeChat, mientras que la mensajería tradicional de SMS y MMS solo representa alrededor del 3 % de los mensajes».

[6] También engloba el acceso a las comunicaciones con poco retardo, como se explica más detenidamente en el informe final del Grupo de Alto Nivel.

El Grupo de Alto Nivel formuló varias recomendaciones, en particular para hacer que las solicitudes de interceptación legal sean aplicables a todos los tipos de proveedores de servicios de comunicaciones electrónicas. Las recomendaciones incluyen aclarar la definición y el ámbito de aplicación de la interceptación legal, determinar las garantías necesarias, aclarar el concepto de competencia territorial sobre los datos, estudiar la manera en que la orden europea de investigación podría apoyar mejor la eficiencia de las solicitudes de interceptación legal transfronterizas y fomentar el desarrollo de acuerdos bilaterales sobre el acceso en tiempo real a datos con terceros países. A más largo plazo, sobre la base de nuevos análisis y de una evaluación de impacto, los expertos recomendaron la elaboración de un instrumento de la UE sobre la interceptación legal (consistente en instrumentos no vinculantes o vinculantes) con fines de orden público que establezca obligaciones exigibles para los proveedores de servicios de comunicaciones electrónicas en la UE.

En su hoja de ruta, la Comisión señaló su intención de proponer medidas destinadas a mejorar la eficiencia de las solicitudes transfronterizas, reforzando los instrumentos existentes, como la orden europea de investigación (de aquí a 2027), y de estudiar medidas para crear unas condiciones de competencia equitativas para todos los tipos de proveedores de comunicaciones, determinando el enfoque más eficiente para hacer frente a los proveedores de comunicaciones no cooperativos.

Durante la Presidencia danesa, se invitará a los Estados miembros a intercambiar información sobre sus prácticas y las limitaciones que experimentan actualmente para aplicar medidas de interceptación legal transfronteriza, en particular en el contexto de la orden europea de investigación y los acuerdos bilaterales y multilaterales.

3. El desafío horizontal del cifrado

También es importante insistir en el desafío que el cifrado representa para el acceso a los datos para una investigación penal eficaz, en particular en lo relativo a la conservación de datos y la interceptación legal ya mencionadas. Hoy en día, muchos servicios emplean el cifrado de extremo a extremo para proteger la confidencialidad de las comunicaciones, la privacidad y la ciberseguridad, pero esto puede dificultar enormemente el acceso lícito a datos legibles de comunicaciones por parte de las autoridades policiales.

La Comisión anunció en su hoja de ruta que en 2026 presentará una hoja de ruta tecnológica centrada específicamente en el cifrado con el fin de determinar y evaluar soluciones que permitan acceder de manera lícita a datos cifrados sin menoscabo de la ciberseguridad ni de los derechos fundamentales. Para lograr este objetivo, la Comisión va a crear un grupo de expertos que debería empezar a trabajar en otoño de 2025.

Asimismo, la Comisión apoyará la investigación y el desarrollo de nuevas capacidades de descifrado para dotar a Europol de capacidades de descifrado de próxima generación (a partir de 2030).

Próximos pasos y coordinación

La cuestión del acceso a los datos para una investigación penal eficaz es compleja y requiere un planteamiento multidisciplinar. En aras de la eficiencia de los trabajos futuros y para garantizar que se tengan en cuenta todos los aspectos, la Presidencia danesa considera esencial contar con la participación de los distintos órganos preparatorios del Consejo, en particular los que se encargan de la seguridad interior y de la cooperación policial, de la cooperación en materia penal y de la ciberseguridad. En las Conclusiones del Consejo de 12 de diciembre de 2024, el Consejo encomendó al Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI), en colaboración con el Comité de Coordinación en el ámbito de la Cooperación Policial y Judicial en Materia Penal (CATS), que coordinara, debatiera y supervisara la aplicación de la hoja de ruta. La Presidencia danesa elaboró un compendio detallado de las actividades previstas en el ámbito del acceso a los datos para una aplicación eficaz de la ley, con un reparto de tareas y un calendario, que el COSI examinó el 18 de septiembre de 2025[7].

La Presidencia danesa considera muy importante continuar velando por que tanto los ministros de Interior como los ministros de Justicia sigan de cerca la evolución del acceso a los datos para una aplicación eficaz de la ley, con el objetivo de dotar a las autoridades competentes de las herramientas que son necesarias para enjuiciar eficazmente los delitos sin menoscabo de los derechos fundamentales. Con este fin, al término de la Presidencia se elaborará una nota informativa dirigida al Consejo en la que se señalarán las actividades llevadas a cabo en las distintas estructuras del Consejo.

---

[7] 12381/25.