COMISIÓN
EUROPEA

Bruselas, 11.12.2025
COM(2025) 752 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

en el que se evalúa y valora el impacto operativo de la aplicación de las funciones previstas en el Reglamento (UE) 2022/991, en particular, el artículo 4, apartado 1, letra t), el artículo 18, apartado 2, letra e), el artículo 18, apartado 6 bis, y los artículos 18 bis, 26, 26 bis y 26 ter, en relación con los objetivos de Europol, así como el impacto de dichas tareas en los derechos y libertades fundamentales consagrados en la Carta, de conformidad con el artículo 68, apartado 3, del Reglamento (UE) 2016/794

{SWD(2025) 404 final}

1. Objeto de la evaluación

Desde que comenzó a funcionar en 1999, **la Agencia de la Unión Europea para la Cooperación Policial (Europol)** ha desempeñado **un papel central en la lucha contra los delitos de especial gravedad con una dimensión transfronteriza y el terrorismo**, convirtiéndose en un motor clave de la cooperación policial en Europa. El panorama de la seguridad ha experimentado cambios drásticos en los últimos treinta años, con el consiguiente cambio en la esencia misma de la delincuencia grave y organizada[1]. Los Estados miembros presentan nuevas necesidades operativas para hacer frente a las amenazas emergentes de manera eficaz, y sus **expectativas de ayuda por parte de Europol** también **han evolucionado**. Por consiguiente, el mandato de Europol ha sido sustituido o modificado en varias ocasiones para mantener y mejorar la pertinencia de la Agencia.

El mandato de Europol, tal como se establece en el Reglamento (UE) 2016/794[2] (en lo sucesivo, el «Reglamento Europol»), fue modificado por última vez en 2022 por el Reglamento (UE) 2022/991[3] a fin de hacer frente a nuevas amenazas para la seguridad. El Reglamento Europol ya no era adecuado para su finalidad en una nueva realidad, en la que los delincuentes aprovechan las ventajas de la **transformación digital**, las **nuevas tecnologías**, la **globalización** y la **movilidad**[4].

Los **objetivos específicos** del Reglamento (UE) 2022/991[5] eran:

- permitir una cooperación efectiva entre las **entidades privadas** y las autoridades policiales para luchar contra el uso indebido de los servicios transfronterizos por parte de los delincuentes;
- permitir que las autoridades policiales analicen **conjuntos de datos grandes y complejos** para detectar vínculos transfronterizos, respetando plenamente los **derechos fundamentales**;
- permitir a los Estados miembros el uso de las **nuevas tecnologías** con fines coercitivos.

Además, el Reglamento (UE) 2022/991 modificó las normas de protección de datos aplicables a Europol para mantener un **elevado nivel de protección de datos,** logrando un equilibrio entre las nuevas competencias de la Agencia para el tratamiento de los datos personales y la privacidad y la protección de los datos personales de las personas. Por otro lado, armonizó en gran medida las normas de protección de datos aplicables a Europol con las aplicables a otras agencias y organismos de la Unión Europea (UE) en materia de Justicia y Asuntos de Interior (JAI) en virtud del capítulo IX del Reglamento (UE) 2018/1875 («Reglamento de protección de datos de la UE»), y las aplicables a las autoridades policiales de los Estados miembros («autoridades competentes») en virtud de su legislación nacional por la que se transporte la

---

1 Europol, *2025 EU Serious and Organised Crime Threat Assessment (SOCTA) — The changing DNA of serious and organised crime*, [«Evaluación de la amenaza de la delincuencia grave y organizada de la Unión Europea: cambio en la esencia misma del crimen grave y organizado», documento en inglés] disponible en línea en https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf («EU SOCTA 2025»). Véase también la evaluación de amenazas aduaneras (CTA, por sus siglas en inglés) de 2025, disponible en línea en https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 DO L 135 de 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 DO L 169 de 27.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final, de 9 de diciembre de 2020, p. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Véase la nota anterior.*

Directiva (UE) 2016/680 («Directiva sobre protección de datos en el ámbito penal»)[6], a fin de **facilitar el flujo de información**.

El presente informe se ha adoptado de conformidad con la obligación de la Comisión, en virtud del **artículo 68, apartado 3, del Reglamento Europol**, para evaluar[7] y valorar los efectos operativos de las funciones de Europol establecidas en el Reglamento (UE) 2022/991 tres años después de su entrada en vigor. Con arreglo al mandato de los colegisladores, la Comisión: en primer lugar, evaluó y valoró los **efectos operativos** de algunas de las nuevas normas para el tratamiento de datos personales, en relación con los objetivos de Europol, en virtud del artículo 3 del Reglamento Europol (a saber: apoyar y reforzar la acción de las autoridades competentes de los Estados miembros y su cooperación mutua en la prevención y la lucha contra las infracciones penales incluidas en el mandato de Europol); en segundo lugar, evaluó el impacto de dichas normas en los **derechos y libertades fundamentales** (en lo sucesivo, «derechos fundamentales») consagrados en la Carta de los Derechos Fundamentales de la Unión Europea[8] y, en tercer lugar, llevó a cabo un **análisis de costes y beneficios** de las funciones relacionadas con el tratamiento de datos.

Para preparar la revisión, los servicios de la Comisión recabaron información y comentarios de diversas fuentes y celebraron consultas *ad hoc* con Europol y los Estados miembros. El **documento de trabajo de los servicios de la Comisión** adjunto ofrece una descripción detallada del contexto general y la metodología de la revisión, así como una descripción exhaustiva de las fuentes de pruebas y consultas que corroboran las principales conclusiones resumidas en el presente informe.

2. Contexto general

De conformidad con el artículo 68, apartado 3, del Reglamento Europol, el presente informe de la Comisión abarca determinadas disposiciones del Reglamento (UE) 2022/991, y se centra en cinco aspectos clave del trabajo de Europol.

1) Dimensión exterior: artículo 4, apartado 1, letra t), del Reglamento Europol sobre las descripciones de información del Sistema de Información de Schengen (SIS) relativas a nacionales de terceros países a propuesta de Europol

Dado el **carácter global de la delincuencia grave y el terrorismo**, la información en poder de terceros países y organizaciones internacionales sobre los autores y las personas sospechosas de tales delitos es cada vez más pertinente para la seguridad interior de la UE. Por lo tanto, la dimensión exterior de la cooperación policial de la UE se ha vuelto crucial para los Estados miembros, al igual que el **papel de Europol a la hora de apoyar a los Estados miembros en sus asociaciones con terceros países** o con entidades situadas en dichos países. **En el futuro, serán esenciales nuevos esfuerzos** para reforzar la seguridad a nivel mundial[9].

El Reglamento (UE) 2022/991 ya introdujo modificaciones sustanciales en el Reglamento Europol con el fin de reforzar la **dimensión exterior de las actividades de Europol**, en

---

6 DO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

7 Esta evaluación realizada de conformidad con el artículo 68, apartado 3, del Reglamento Europol no es la evaluación que debe llevarse a cabo de conformidad con las directrices para la mejora de la legislación con vistas a una posible propuesta de revisión de dicho Reglamento. Véase también la sección 4 a continuación.

8 Carta de los Derechos Fundamentales de la Unión Europea. DO C 326 de 26.10.2012, p. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

9 Véase «ProtectEU: una Estrategia Europea para la Seguridad Interior», COM(2025) 148 final, de 1 de abril de 2025, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52025DC0148.

particular facilitando el intercambio de información con terceros países[10] y solicitando a Europol que incluya una estrategia para las relaciones con terceros países y organizaciones internacionales en su programación plurianual y sus programas de trabajo anuales[11].

El **artículo 4, apartado 1, letra t), del Reglamento Europol** asigna una nueva función a Europol: apoyar a los Estados miembros en el tratamiento de datos sobre personas implicadas en actos de terrorismo o delitos graves facilitados por terceros países u organizaciones internacionales. Esto incluye **proponer a los Estados miembros la posible introducción de descripciones de información sobre nacionales de terceros países en interés de la Unión en el Sistema de Información de Schengen (SIS)**. Esta nueva categoría de descripciones de información se introdujo en 2022[12], a raíz de una modificación del Reglamento (UE) 2018/1862 relativo a la utilización del SIS en el ámbito de la cooperación policial y judicial en materia penal[13].

Existe determinada información, especialmente cuando la persona en cuestión no es un ciudadano de la UE y no existe relación con un caso nacional, que el tercer país comparte únicamente con Europol, que trata los datos y comparte los resultados de su análisis con todos los Estados miembros. El objetivo de las nuevas disposiciones era **maximizar la explotación de la información** que Europol recibe de terceros países, haciéndola más accesible que si solo estuviera disponible a través del propio sistema de Europol. Complementó otras medidas, como el portal europeo de búsqueda (PEB) y el marco de interoperabilidad[14] entre los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, abordando las deficiencias estructurales relacionadas con dichos sistemas que impiden el trabajo de las autoridades nacionales y, en particular, de la guardia de fronteras.

El **SIS** se considera un **canal de difusión adicional clave**: es la base de datos más utilizada en Europa para la aplicación de la ley, el control fronterizo y la migración. En 2024, se realizaron más de 15 000 millones de búsquedas en el SIS, frente a aproximadamente 14 millones de búsquedas en el sistema de información de Europol (SIE) y menos de 3 000 millones de búsquedas (en todo el mundo) en las 19 bases de datos de Interpol, que son los otros dos principales sistemas de información para las autoridades competentes[15].

2) Innovación: artículo 18, apartado 2, letra e), y artículo 33 *bis* del Reglamento Europol sobre el tratamiento de datos personales por parte de Europol para proyectos de innovación e investigación

---

10 Véase, por ejemplo, el artículo 25, apartado 4 *bis*, del Reglamento Europol, que ofrece a Europol la posibilidad de transferir datos a terceros países tras haber realizado una autoevaluación de todas las circunstancias que concurren en la transferencia de datos personales y haber llegado a la conclusión de que existen garantías adecuadas con respecto a la protección de datos personales, y el artículo 25, apartado 5, del Reglamento Europol, que amplía el ámbito de aplicación de los casos excepcionales en los que Europol puede realizar una transferencia o una categoría de transferencias *ad hoc* en casos debidamente justificados a terceros países y organizaciones internacionales.

11 Artículo 12, apartado 2, del Reglamento Europol.

12 Reglamento (UE) 2022/1190. DO L 185 de 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Reglamento (UE) 2018/1862. DO L 312 de 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Reglamento (UE) 2019/818. DO L 135 de 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 Informe anual del SIS 2024 de eu-LISA, disponible en línea en https://www.eulisa.europa.eu/our-publications/sis-annual-statistics-report-2024-factsheet; Europol, *Consolidated Annual Activity Report* (CAAR) de 2024, disponible en línea en https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF; y https://www.interpol.int/es/Como-trabajamos/Bases-de-datos.

Los avances tecnológicos presentan grandes oportunidades y también retos considerables para la seguridad interior[16] de la UE, y han tenido un impacto tan profundo en la delincuencia como para alterar incluso la naturaleza misma, el ADN, de las amenazas graves y de la delincuencia organizada[17]. Los delincuentes integran con gran rapidez las nuevas tecnologías en sus operaciones, creando nuevos modelos de negocio y perfeccionando sus tácticas. Al mismo tiempo, estos avances ofrecen **oportunidades sin precedentes para que las autoridades policiales mejoren sus capacidades**. Por lo tanto, la investigación y la innovación desempeñan un papel crucial en la seguridad interior mediante el desarrollo de soluciones para contrarrestar las amenazas emergentes y seguir el ritmo de la rápida evolución de las formas y *modus operandi* de las redes delictivas, incluidas las derivadas del uso indebido de la tecnología. La Unión ha invertido, y seguirá invirtiendo, en el desarrollo de herramientas innovadoras a través de la investigación y la innovación en materia de seguridad financiadas por la UE, en el marco de **ProtectEU** (Estrategia Europea para la Seguridad Interior)[18].

Creado a finales de 2019, por mandato de los ministros de Justicia y Asuntos de Interior (JAI) de los Estados miembros de la UE, el **Laboratorio de Innovación de Europol**[19] (EIL, por sus siglas en inglés) tiene por objeto impulsar el compromiso de Europol con la innovación en el ámbito policial. El Reglamento (UE) 2022/991 introdujo modificaciones sustanciales en el Reglamento Europol para reforzar el mandato de Europol en materia de innovación, a fin de apoyar el potencial del EIL y promover sinergias con otras actividades de investigación e innovación a escala de la UE, en especial en la Comisión, en el marco del **Centro de Innovación de la UE** para la Seguridad Interior[20].

El artículo 18, apartado 2, del Reglamento Europol, sobre los fines de las actividades de tratamiento de la información, se modificó para permitir a Europol **tratar datos personales operativos** también **para proyectos de investigación e innovación**. La disponibilidad de conjuntos de datos de alta calidad que permitan la verificación empírica de la validez de las nuevas herramientas se considera en general una condición previa clave para el desarrollo de tecnologías. Por el contrario, unos conjuntos de datos poco fiables o sesgados para pruebas pueden dar lugar al desarrollo de tecnologías deficientes[21].

En el artículo 18, apartado 3 *bis*, el artículo 30, apartados 2 y 3, y el artículo **33 *bis* del Reglamento Europol** se establecieron salvaguardias específicas en materia de protección de datos para dicho tratamiento. El artículo 33 *bis* exigía la creación de un **entorno controlado de pruebas** estipulando que todos los datos personales tratados en el contexto de un proyecto deben copiarse temporalmente en un entorno de tratamiento de datos separado, aislado y protegido dentro de Europol para su uso exclusivo para dicho proyecto.

3) <u>Investigaciones penales</u>: artículo 18, apartado 6 *bis*, y artículo 18 *bis* del Reglamento Europol sobre las condiciones para el tratamiento de los datos personales recibidos sin categorización de los interesados (DSC)

En su papel de **centro de información penal de la UE**, Europol no solo facilita la recogida y el intercambio de información, sino que también contribuye a **aumentar la eficacia de las investigaciones mediante el análisis avanzado de datos** y la detección de vínculos entre las

16 Europol, Evaluación de la amenaza de la delincuencia organizada en internet (IOCTA) 2024, disponible en línea en Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

17 Europol, EU SOCTA 2025, p. 19.

18 COM(2025) 148 final, de 1 de abril de 2025, p. 9: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52025DC0148.

19 https://www.europol.europa.eu/how-we-work/innovation-lab.

20 Véase, en particular, el artículo 4, apartado 1, letras v) y w), del Reglamento Europol.

21 SWD(2020) 543 final, de 9 de diciembre de 2020, p. 29.

infracciones penales y las redes delictivas a través de las fronteras que no son visibles a nivel nacional. Estas capacidades ayudan a los Estados miembros al ampliar la información disponible para sus investigaciones penales.

Con el uso cada vez más amplio e intensivo de la tecnología, los **conjuntos de datos grandes y complejos han pasado a ser totalmente normales en todos los aspectos de la vida**, incluida la delincuencia[22]. Las investigaciones sobre la delincuencia organizada o el terrorismo han empezado a enfrentarse al reto de analizar grandes volúmenes de datos almacenados electrónicamente, que a menudo equivalen a terabytes, incluidos datos de audio, vídeo y datos generados por máquinas incautados durante las investigaciones. Por ejemplo, en la investigación conjunta para desmantelar la red EncroChat[23], los investigadores analizaron millones de mensajes que los delincuentes intercambiaron para planificar delitos graves. En este contexto, la disponibilidad de las herramientas, los conocimientos especializados y los recursos necesarios en el ámbito de las tecnologías de la información y de las comunicaciones (TIC) para analizar conjuntos de datos grandes y complejos (conocidos en el lenguaje técnico común como «macrodatos»[24]) es clave para las autoridades policiales y judiciales.

Aunque el Reglamento Europol adoptado en 2016 no imponía restricciones como tales al análisis de macrodatos, sí carecía de disposiciones estructuradas que establecieran las condiciones para el análisis de este tipo de datos. El **punto más crítico** fue el **requisito relativo a la categorización de los interesados**. La categorización de los interesados se refiere a la necesidad de examinar los conjuntos de datos para clasificar los datos personales en función de diferentes categorías, que se enumeran exhaustivamente en los anexos II.A y II.B del Reglamento Europol, antes de proceder al tratamiento efectivo de los datos con fines de investigación, incluso antes de cotejar datos para detectar vínculos o de llevar a cabo análisis de carácter estratégico o temático o análisis operativos[25]. Las categorías pertinentes están vinculadas a diferentes tipos de participación en investigaciones penales, incluidos: i) sospechosos y posibles delincuentes futuros; así como ii) contactos, socios, víctimas, testigos e informantes asociados a actividades delictivas. Por lo general, Europol no puede tratar, ni siquiera almacenar, los datos personales de personas que no pertenecen a ninguna de estas categorías.

Los proveedores de datos, como los **Estados miembros** o los **organismos y agencias de la UE**, **por lo general** ya categorizan a los interesados antes de transferir los datos personales a Europol[26]. En virtud del Derecho de la Unión, todos ellos están obligados a categorizar a los interesados para su propio tratamiento e investigaciones, independientemente de la transferencia de datos a Europol, y sobre la base de normas equivalentes, aunque no idénticas,

---

22 Europol, EU SOCTA 2025, *passim*.

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 Supervisor Europeo de Protección de Datos, Dictamen 7/2015, p. 7, disponible en https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. «En términos generales, como denominador común de las diversas definiciones disponibles, los "**macrodatos**" se refieren a la práctica de combinar grandes volúmenes de información procedente de fuentes distintas y analizarlos, utilizando algoritmos más sofisticados para fundamentar las decisiones. Los macrodatos no solo se basan en la creciente capacidad de la tecnología para respaldar la recogida y el almacenamiento de grandes cantidades de datos, sino también en su capacidad para analizar, comprender y aprovechar todo su valor (en concreto, utilizando aplicaciones analíticas)».

25 Véase el artículo 18, apartado 2, del Reglamento Europol.

26 Los Estados miembros transfieren datos a Europol a través de su Aplicación de la Red de Intercambio Seguro de Información (SIENA), en la que la categorización de interesados se aplica como campo obligatorio.

a las de Europol[27]. Sin embargo, en el caso de conjuntos de datos grandes y complejos, el tratamiento previo manual es una práctica que requiere recursos y mucho tiempo. El análisis de los datos en un solo teléfono móvil puede llevar, de manera semiautomatizada, hasta tres días, y durante una investigación pueden incautarse hasta cientos de teléfonos móviles. La categorización de los interesados para **macrodatos no siempre es posible**, dado el gran volumen de los conjuntos de datos, la forma en que los datos están estructurados, la falta de recursos o el excesivo **esfuerzo manual necesario**. En la práctica, la única posibilidad es analizar primero los datos con mayor profundidad desde un punto de vista operativo, o detectar vínculos, incluso de forma semiautomatizada, cotejando los datos disponibles.

El Reglamento (UE) 2022/991 aclaró las condiciones para que la categorización de interesados proporcione **seguridad jurídica** en relación con el tratamiento de conjuntos de datos grandes y complejos. Europol y el Supervisor Europeo de Protección de Datos (SEPD) interpretaron de manera diferente la letra y el espíritu del Reglamento Europol en lo que respecta al período de conservación de datos aplicable. Según Europol, dicho período debería ser de tres años; según el SEPD, debería ser de seis meses[28]. También fueron necesarias nuevas disposiciones para ofrecer una **mayor flexibilidad**, logrando un equilibrio adecuado entre la protección de datos y los aspectos relativos a la seguridad.

El artículo 18, apartado 5 *bis*, del Reglamento Europol, en combinación con el artículo 73 del Reglamento de protección de datos de la UE, aclaró en primer lugar el principio general de la categorización de interesados en virtud del artículo 18, apartado 2, y del anexo II. Europol tiene la tarea, cuando proceda y en la medida de lo posible, de **asignar claramente los datos personales a una categoría específica de interesados**. En la práctica, Europol debe determinar, por regla general, el papel exacto en la actividad delictiva (por ejemplo, si una persona es un sospechoso, una víctima o solo un testigo) de cada persona cuyos datos personales serán tratados y no a nivel agregado para todas las personas de un fichero que deba tratarse, o parte de él (por ejemplo, simplemente estableciendo que todas las personas mencionadas están implicadas en una actividad delictiva comprendida en su mandato sobre la base de un examen de las circunstancias generales que generaron el fichero de datos) antes de que puedan tratarse los datos personales.

El artículo 18, apartado 6 *bis*, del Reglamento Europol permite explícitamente el tratamiento de los datos personales recibidos sin categorización de interesados durante un **máximo de dieciocho meses**, que puede prorrogarse hasta treinta y seis meses en casos justificados, únicamente con el **fin de completar la categorización de interesados**. El artículo 18, apartado 6 *bis*, del Reglamento Europol no hace referencia explícita a conjuntos de datos grandes y complejos, sino que, de manera más general, requiere que sea «**estrictamente necesario**».

El artículo 18 *bis* del Reglamento Europol establece una excepción al permitir a Europol tratar los datos personales recibidos de una **autoridad competente**, de la **Fiscalía Europea** o de **Eurojust**, cuando sea necesario para apoyar una **investigación penal en curso**, sin necesidad de realizar una categorización de los interesados, si aún no se ha realizado, y más allá de las categorías de interesados enumeradas en el Reglamento Europol. Europol puede tratar los datos

---

27 Véase, por ejemplo, el artículo 6 de la Directiva (UE) 2016/680 (la «Directiva sobre protección de datos en el ámbito penal» en lo que respecta a las autoridades indirectamente competentes); DO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; artículo 51 del Reglamento (UE) 2017/1939 del Consejo (en lo sucesivo, «Reglamento sobre la Fiscalía Europea»); DO L 283 de 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; artículo 27, apartado 3, del Reglamento (UE) 2018/1727 (en lo sucesivo, «Reglamento sobre Eurojust»); DO L 295 de 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

28 https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

mediante **análisis operativos** o, en casos excepcionales y debidamente justificados, mediante **controles cruzados** para identificar conexiones u otros vínculos pertinentes. Esta excepción se concibió para abordar las diferencias entre las normas relativas a la categorización de los interesados aplicables a Europol y las aplicables a las autoridades competentes, la Fiscalía Europea y Eurojust.

4) Cooperación con terceros: artículos 26, 26 *bis* y 26 *ter* del Reglamento Europol sobre el intercambio de datos personales entre Europol y entidades privadas

Los delincuentes abusan cada vez más de los servicios (transfronterizos) de entidades privadas, tales como servicios a través de internet, financieros y de telecomunicaciones tradicionales. Por consiguiente, las **entidades privadas poseen una gran cantidad de datos personales pertinentes para las investigaciones penales**. En particular, internet ha creado un espacio público que, en la práctica, está en manos privadas, lo que dificulta el cumplimiento de las normas en línea con fines policiales con la misma eficacia que fuera de línea[29].

En este contexto, la **cooperación entre las autoridades policiales y las entidades privadas** se ha vuelto **indispensable**. Tal como se establece en la Estrategia Europea para la Seguridad Interior, **ProtectEU**, será esencial reforzar las asociaciones con el sector privado para facilitar el intercambio de información[30]. Los jefes de policía también han pedido, en su declaración conjunta sobre el futuro de Europol[31], que Europol actúe como una «**puerta de acceso vital para obtener información de entidades privadas**». La naturaleza de esta colaboración va desde el intercambio de información y la provisión de datos comerciales de código abierto, hasta la participación en proyectos de investigación e innovación y la prestación de servicios que apoyen el funcionamiento de las empresas[32]. Por ejemplo, en 2025, Europol neutralizó con éxito LummaStealer, la amenaza de robo de información más importante del mundo, a través de la cooperación con Microsoft, que había identificado más de 394 000 ordenadores Windows infectados a escala mundial por el software malicioso Lumma[33].

El Reglamento (UE) 2022/991 introdujo **posibilidades adicionales** para que Europol intercambiara datos personales con entidades privadas. Antes de ello, Europol solo podía recibir datos personales de entidades privadas a través de una unidad nacional de Europol, o a través de puntos de contacto o autoridades de terceros países u organizaciones internacionales previamente identificados. La finalidad del tratamiento por parte de Europol se limitaba a identificar la unidad nacional de Europol pertinente, o el punto de contacto del tercer país y la organización internacional o la autoridad que pudiera asumir la responsabilidad del caso.

El **artículo 26 modificado del Reglamento Europol amplió la labor de Europol**, permitiéndole tratar la información (en particular los datos personales) procedente de entidades privadas de forma exhaustiva. Uno de los objetivos principales del tratamiento ha seguido siendo la identificación de la unidad nacional de Europol en cuestión. No obstante, Europol

---

29 SWD(2020) 543 final, de 9 de diciembre de 2020, pp. 16-17.

30 Véase «ProtectEU: una Estrategia Europea para la Seguridad Interior», p. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Cooperación con entidades privadas, 31 de mayo de 2023, EDOC #1306090v13. Véase también Milieu Consulting, *Study on the Practice of direct exchange with of personal data between Europol and Private parties*, [«Estudio sobre la práctica del intercambio directo de datos personales entre Europol y entidades privadas», documento en inglés] informe final, septiembre de 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. En el documento de trabajo adjunto de los servicios de la Comisión se ofrecen otros ejemplos.

también está autorizada ahora a completar la información con su propio análisis para facilitar el tratamiento ulterior de un caso a nivel nacional.

Además de las disposiciones horizontales del artículo 26 del Reglamento Europol, el artículo 26 *bis* introdujo normas para las **situaciones de crisis en línea** y el artículo 26 *ter* aborda la **difusión de material de abuso sexual de menores en línea**. En tales casos, Europol podrá ayudar a los Estados miembros mediante el tratamiento de datos personales recibidos directamente de entidades privadas. Europol también podrá transmitir datos personales a entidades privadas caso por caso.

El Reglamento (UE) 2022/991 introdujo la posibilidad de utilizar la infraestructura de Europol para el intercambio de información entre las autoridades competentes y las entidades privadas, así como la posibilidad de que Europol solicite a los Estados miembros que obtengan, de conformidad con su legislación nacional, datos personales de entidades privadas.

Estas disposiciones se adoptaron en consonancia con otras iniciativas, como el Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea[34] y el Reglamento de Servicios Digitales[35]. Se prevén nuevas medidas para mejorar la participación de las entidades privadas en la lucha contra la delincuencia y para facilitar el acceso lícito a los datos con el fin de lograr «la ambición de un cambio de cultura en lo que respecta a la seguridad» (**enfoque que implica a toda la sociedad**) en el marco de **ProtectEU**[36].

5) Supervisión interna y externa del respeto de los derechos fundamentales por parte de Europol

El Reglamento (UE) 2022/991 hace hincapié en la obligación de Europol de respetar los derechos fundamentales en virtud de las disposiciones que definen las funciones de Europol y la mejora de las salvaguardias conexas, en particular **mediante el refuerzo de la supervisión interna y externa de la Agencia**.

En el ámbito de la protección de datos, la adaptación del Reglamento Europol a las garantías de protección de datos en virtud del Reglamento de protección de datos de la UE implicaba la introducción de nuevas normas para la supervisión por parte del **responsable de la protección de datos** (RPD) y del **Supervisor Europeo de Protección de Datos** (SEPD). Por ejemplo, la obligación de proporcionar una evaluación de impacto relativa a la protección de datos y la consulta previa al SEPD se han convertido en prácticas sistemáticas para cualquier nuevo tipo de tratamiento. El Reglamento (UE) 2022/991 también introdujo una nueva competencia de Europol para las solicitudes de derechos de acceso. Antes de eso, las autoridades nacionales competentes eran responsables de tramitar las solicitudes de derechos de acceso si los Estados miembros eran los proveedores de datos.

El Reglamento (UE) 2022/991 también estableció un **nuevo puesto de agente de derechos fundamentales** en Europol, encargado, entre otras cosas, de informar al director ejecutivo de Europol sobre posibles violaciones de los derechos fundamentales en el transcurso de las actividades de la Agencia.

Además, el **control democrático y la rendición de cuentas se reforzaron** mediante el seguimiento político de las actividades de Europol por parte del **Parlamento Europeo y los Parlamentos nacionales**, tal como se establece en el artículo 88, apartado 2, párrafo segundo, del Tratado de Funcionamiento de la Unión Europea (TFUE). El Reglamento (UE) 2022/991

---

34 Reglamento (UE) 2021/784. DO L 172 de 17.5.2021, p. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

35 Reglamento (UE) 2022/2065. DO L 277 de 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

36 Véase «ProtectEU: una Estrategia Europea para la Seguridad Interior», p. 2.

también reforzó el seguimiento por parte del **Grupo de Control Parlamentario Conjunto** (GCPC)[37]. Por ejemplo, preveía la consulta obligatoria del GCPC en lo que respecta al proyecto de programación plurianual y el programa anual de trabajo de Europol, la posibilidad de que el GCPC dirigiera recomendaciones específicas no vinculantes a Europol y las presentara al Parlamento Europeo y a los Parlamentos nacionales, y la creación de un foro consultivo para asistir al GCPC, previa petición, mediante un asesoramiento independiente en materia de derechos fundamentales.

3. Principales conclusiones de la evaluación

3.1. Situación de la aplicación operativa de las nuevas competencias y funciones de Europol en materia de tratamiento de datos personales

El Reglamento (UE) 2022/991 entró **en vigor el 28 de junio de 2022**. Sin embargo, su aplicación operativa dependía de diversas medidas de gobernanza, técnicas y administrativas, así como de requisitos operativos, como la creación de nuevas estructuras de TIC en algunos casos.

Tres años después, **casi todas las disposiciones** enumeradas en el artículo 68, apartado 3, del Reglamento (UE) 2022/991 **han entrado en vigor**. Las disposiciones relativas al análisis de conjuntos de datos grandes y complejos (artículo 18, apartado 6 *bis*, y artículo 18 *bis* del Reglamento Europol) y a la cooperación con entidades privadas (artículos 26, 26 *bis* y 26 *ter* del Reglamento) comenzaron a aplicarse a partir del 28 de junio de 2022, o poco después. El tratamiento de datos personales para proyectos de investigación e innovación [artículo 18, apartado 2, letra e), del Reglamento Europol] comenzó en 2023 después de que el entorno controlado de pruebas, denominado ODIN, se estableciera para cumplir los requisitos específicos de protección de datos en virtud del artículo 33 *bis* del Reglamento Europol. A 29 de junio de 2025, la posibilidad de que Europol propusiera **descripciones de información en el SIS** a los Estados miembros de conformidad con el artículo 4, apartado 1, letra t), del Reglamento Europol aún no había entrado en funcionamiento, ya que la aplicación técnica del nuevo tipo de descripción sigue en curso. La entrada en funcionamiento está **prevista para 2026**.

3.2. Evaluación de los efectos operativos de las nuevas competencias y funciones de Europol en materia de tratamiento de datos personales en los objetivos de la Agencia en virtud del artículo 3 del Reglamento Europol

Por lo que se refiere a los efectos operativos de las nuevas competencias y funciones de Europol en materia de tratamiento de datos personales, la consulta indicó que, **en general, los Estados miembros mantienen una opinión favorable** sobre su pertinencia, eficacia y valor añadido, así como del apoyo de Europol a sus autoridades competentes en los ámbitos conexos[38].

Las competencias de investigación contempladas por esta evaluación no se utilizan de forma continua o sistemática para tratar datos con fines de seguimiento; algunas de ellas son incluso de carácter excepcional, mientras que otras se utilizan con mayor regularidad en función de las necesidades en las investigaciones. El **uso operativo de las nuevas disposiciones** durante el período de referencia **difería significativamente** en **términos cuantitativos**, dependiendo de

[37] Véase https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

[38] Véanse las pruebas presentadas en la sección 5 del documento de trabajo de los servicios de la Comisión que acompaña al presente informe, y en particular las observaciones de Europol y las respuestas de los Estados miembros a las preguntas 2, 4 y 5 del cuestionario breve de 2 de junio de 2025, en el anexo III del documento de trabajo de los servicios de la Comisión.

las distintas características técnicas y condiciones jurídicas asociadas a las nuevas disposiciones.

Europol recibió un número **nada desdeñable** de **nuevas contribuciones sin categorización de los interesados** procedentes de los Estados miembros en virtud del artículo 18, apartado 6 *bis*, del Reglamento Europol, que ascendieron a 653 en 2023 y 597 en 2024. Por otro lado, no se produjo un aumento a corto plazo de las contribuciones sin categorización de los interesados, y el número de casos en los que se aplicó el artículo 18, apartado 6 *bis*, se mantuvo **estable** en comparación con casos equivalentes en el período anterior al 28 de junio de 2022. Las nuevas disposiciones tampoco tuvieron un impacto negativo en el compromiso de los Estados miembros de llevar a cabo la categorización de los interesados[39]. Entre 2023 y 2024, el porcentaje de contribuciones sin categorización de los interesados representó **menos del 1 % de todas las contribuciones** aceptadas por Europol de los Estados miembros (0,85 % en 2023 y 0,71 % en 2024). Desde junio de 2022, Europol ha completado sistemáticamente la categorización de los interesados en un plazo de dieciocho meses, sin hacer uso del plazo ampliado de treinta y seis meses. Europol y seis Estados miembros pusieron de relieve que, a pesar de la mejora de la seguridad jurídica, la **carga administrativa seguía siendo significativa** tanto para Europol como para las autoridades competentes debido al esfuerzo necesario para cumplir con la categorización de los datos personales mediante la participación individual en la infracción penal. Europol aplica este requisito de forma muy estricta[40].

Europol informó de que el intercambio de información con **entidades privadas** seguía siendo insignificante en 2023, ya que solo se registraron veintiséis casos de aplicación del artículo 26 del Reglamento Europol (además de los casos que entran en el ámbito de aplicación del Reglamento de Servicios Digitales)[41]. Sin embargo, en **2024**, las estadísticas mostraron un **fuerte aumento hasta los 284** (casi un 1 000 % más) casos que implicaban cooperación con entidades privadas en virtud del artículo 26 del Reglamento Europol. Este fue el caso, en particular, de los datos de empresas privadas para la investigación de **delitos financieros y económicos**. Europol también hizo un uso significativo del artículo 26 *ter* del Reglamento Europol en la lucha contra la explotación sexual de menores, en la que la cooperación con entidades privadas ya era muy importante antes de la entrada en vigor del Reglamento. En ambos casos, los datos también incluyen la cooperación que era posible en virtud del marco jurídico anterior. Los datos disponibles no revelan en qué medida estos nuevos casos entran en el ámbito de aplicación de las nuevas disposiciones o responden a un mayor uso de las posibilidades existentes.

En **2025**, Europol adoptó una **nueva estrategia** para seguir mejorando la cooperación con las entidades privadas. Además, se han adoptado medidas para mejorar la infraestructura de TIC de Europol a disposición de las autoridades competentes para el intercambio de información con entidades privadas. En **2023**, Europol puso en marcha la *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**PERCI**) (Plataforma Europea para Retirada de Contenidos Ilícitos en Internet) para facilitar la aplicación del Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea y, en el futuro, posiblemente también del artículo 18 del Reglamento de Servicios Digitales, así como del servicio de notificación de

39 Como subrayó un Estado miembro durante la consulta, «[los Estados miembros] pueden distinguir claramente qué tipo de datos están tratando, lo que puede ser muy importante en la propia investigación».

40 Véase la subsección 7.1.3 del documento de trabajo de los servicios de la Comisión que acompaña al presente informe y las respuestas de los Estados miembros a la pregunta 9 del cuestionario breve de 2 de junio de 2025, en el anexo III del documento de trabajo de los servicios de la Comisión.

41 Europol, Informe de 2023 de conformidad con el artículo 16, apartado 11, del Reglamento Europol.

abuso de menores de la UE **(EU CARES)**. PERCI no está incorporada al Sistema de Información de Europol (SIE)[42].

Otras disposiciones no se utilizaron en absoluto (artículo 26 *bis* del Reglamento Europol), a pesar de estar en vigor, **o** solo se aplicaron **excepcionalmente** (un caso en el que el artículo 18 *bis* del Reglamento se utilizó en 2024 y, en 2025, un proyecto que se llevó a cabo con tratamiento de datos personales con arreglo al artículo 18, apartado 1, letra t), del Reglamento, con tres nuevos proyectos ya en preparación).

Debido al período limitado de aplicación operativa de las disposiciones introducidas por el Reglamento (UE) 2022/991 y a la lentitud propia de las investigaciones penales y los procedimientos judiciales, los Estados miembros no pudieron facilitar datos cuantitativos sobre el impacto de dichas disposiciones en términos operativos. En su lugar, ofrecieron algunos ejemplos de investigaciones realizadas con éxito que demuestran los **beneficios tangibles de las nuevas posibilidades de investigación en situaciones reales** para las disposiciones ya en uso, a saber, EncroChat, Sky ECC, las redes delictivas con sede en los Balcanes implicadas en el tráfico de cocaína o LummaStealer.

Europol y ocho Estados miembros también señalaron algunos **ámbitos de mejora** para maximizar el uso eficiente y coherente del nuevo marco jurídico y reforzar el papel de Europol en el futuro. Existe la preocupación, en particular por parte de Europol, de que la excesiva complejidad, fragmentación y duración temporal de las disposiciones jurídicas puedan disuadir a los profesionales o a las entidades privadas de utilizar los nuevos instrumentos disponibles. Por su parte, los comentarios de los Estados miembros se refieren más bien a la manera en que Europol aplica restrictivamente las garantías de protección de datos bajo la supervisión del SEPD, lo que podría socavar la eficacia y el valor añadido de ciertas disposiciones.

3.3. Evaluación del impacto de las nuevas competencias y funciones de Europol en materia de tratamiento de datos personales en los derechos fundamentales

La Comisión **no** encontró **ninguna** prueba de **impacto negativo en los derechos fundamentales** derivado del uso operativo de las nuevas competencias para el tratamiento de datos personales derivado del uso limitado que se ha hecho hasta la fecha de las nuevas competencias en materia de tratamiento de datos personales.

Además de aplicar los requisitos específicos de protección de datos asociados a las nuevas competencias en materia de tratamiento de datos personales, Europol ha adoptado progresivamente todas las medidas necesarias para aplicar los nuevos mecanismos horizontales de supervisión relacionados con los derechos fundamentales.

En 2024, el Consejo de Administración de Europol adoptó las normas de ejecución revisadas del RPD como uno de los últimos actos de ejecución necesarios relacionados con el nuevo régimen de protección de datos. Las pruebas recogidas sugieren que Europol y su Consejo de Administración también han garantizado, en cooperación con el RPD de Europol y el SEPD, una **aplicación rigurosa de las nuevas garantías de protección de datos** introducidas en 2022. Este enfoque ha impedido, a primera vista, de manera efectiva cualquier impacto negativo o injerencia derivada del uso inicial de las nuevas competencias de tratamiento de datos personales con los derechos de las personas a la protección de la privacidad y los datos personales. Según los Estados miembros, Europol cuenta actualmente con un **sólido marco jurídico de protección de datos**, que garantiza salvaguardias suficientes para un posible aumento del uso de sus nuevas competencias. Siete Estados miembros también subrayaron que

[42] Reglamento (UE) 2019/818; DO L 135 de 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

este marco **facilita el flujo de información** al aumentar la confianza, aunque todavía hay margen de mejora. Solo uno de los Estados miembros expresó una opinión negativa[43].

Además de los **retos** específicos relacionados con la categorización de los interesados, Europol y cuatro Estados miembros mencionaron como ámbitos de mejora los costes y el tiempo asociados a la **evaluación de impacto relativa a la protección de datos** y la **consulta previa** al SEPD, que en la práctica se llevan a cabo sistemáticamente. Otro reto planteado por seis Estados miembros es la tramitación por parte de Europol de las **solicitudes de acceso de los interesados**, para las que ahora es competente aun en los casos en que un Estado miembro sea el propietario de los datos.

El **primer agente de derechos fundamentales** fue nombrado en diciembre de **2022**. En los dos primeros años de su mandato, **no** ha recibido ni ha presentado **ninguna reclamación** al director ejecutivo. El GCPC ha seguido supervisando de cerca las actividades de Europol y no ha formulado ninguna recomendación desde la entrada en vigor de las nuevas disposiciones. El Parlamento Europeo creó el **Foro Consultivo sobre Derechos Fundamentales del GCPC** en febrero de **2024**.

3.4. Análisis de costes y beneficios de las nuevas competencias y funciones de Europol en materia de tratamiento de datos personales

Dado el estado inicial de aplicación de las disposiciones introducidas por el Reglamento (UE) 2022/991 y la limitada experiencia con ellas, es **prematuro** que la Comisión extraiga conclusiones significativas acerca de las nuevas disposiciones a partir de un **análisis de costes y beneficios**.

Los servicios de la Comisión han recabado información de Europol sobre los costes contraídos hasta la fecha en relación con la aplicación operativa del Reglamento (UE) 2022/991, en lo que respecta a las disposiciones objeto de revisión. Estos costes ascendieron aproximadamente a **25 millones EUR** (alrededor del 5 % de la asignación total a Europol[44]) entre 2022 y 2025, y consistieron fundamentalmente en costes puntuales. Hasta la fecha, los Estados miembros no han contraído nuevos gastos pertinentes relacionados específicamente con el Reglamento (UE) 2022/991.

La **mayoría de los costes** (casi 17 millones EUR) consistieron en inversiones significativas en el **desarrollo de nuevas estructuras de TIC**, en disposiciones de aplicación en materia de investigación e innovación (el entorno de pruebas ODIN) y en sistemas de información para el intercambio de datos personales con entidades privadas (PERCI y EU CARES). Los costes en **recursos humanos**, tanto relacionados con las TIC como con las operaciones, representaron aproximadamente un tercio de los gastos totales (alrededor de 8 millones EUR). Los recursos humanos supondrán los **principales costes recurrentes a largo plazo**.

Cabe señalar que los 8 millones EUR mencionados anteriormente no incluyen los costes en recursos humanos para la unidad de gestión de la información (IMU, por sus siglas en inglés) ni los recursos asociados a medidas de supervisión (anteriores y nuevas) de carácter horizontal y para las que no es posible realizar un desglose a nivel de aplicación de disposiciones específicas. Los costes de estos recursos no son insignificantes. Por ejemplo, en 2023, se estimó que participaron en actividades en **organismos de garantía o supervisión y entidades de supervisión o asesoramiento sesenta equivalentes a jornada completa** (EJC) (casi el **5 %**

---

43 Véanse las respuestas de los Estados miembros a la pregunta 9 del cuestionario breve de 2 de junio de 2025, en el anexo III del documento de trabajo de los servicios de la Comisión.

44 En el mismo período, el presupuesto asignado a Europol ascendió en total a aproximadamente **860 millones EUR** (aumentando progresivamente de 192 millones EUR en 2022 a 241 millones EUR en 2025). Para más información, véase el documento de trabajo de los servicios de la Comisión adjunto.

del personal de Europol). Europol asignó veinticinco EJC a los esfuerzos para responder a la supervisión de la protección de datos y a las acciones de garantía correspondientes. Esto incluye el seguimiento de las recomendaciones del SEPD, así como el trabajo generado en el contexto de las consultas previas para el tratamiento de datos operativos. Dieciséis de estos veinticinco EJC se dedican específicamente a actividades relacionadas con los requisitos del SEPD. En junio de 2025, Europol contaba con un equipo específico de ocho agentes a tiempo completo en el ámbito de la protección de datos, incluido el RPD.

Según Europol y quince Estados miembros, se espera que los **beneficios** de las nuevas competencias y funciones en materia de tratamiento de datos personales, en particular el análisis de conjuntos de datos grandes y complejos, así como la cooperación con entidades privadas, sean significativos y **superen los costes asociados**. Ningún Estado miembro expresó una opinión diferente. Es razonable esperar algunas mejoras de la eficiencia a largo plazo, gracias a las economías de escala y a la disminución de los costes marginales. Un Estado miembro subrayó que «es importante que Europol facilite los recursos informáticos necesarios para proporcionar y seguir desarrollando las herramientas para la aplicación de las nuevas posibilidades previstas en el Reglamento (UE) 2022/991»; esta opinión contó también con el apoyo de otros dos Estados miembros y otras partes interesadas[45].

En opinión de Europol y de cinco Estados miembros, las posibles **deficiencias** en la aplicación también deben abordarse en el **marco de gobernanza, administración y protección de datos existente** para evitar socavar los efectos operativos de las nuevas funciones relativas al tratamiento de datos personales retrasando o restringiendo su uso. Cinco Estados miembros cuestionaron una aplicación demasiado prudente de las normas de protección de datos por parte de Europol y su Consejo de Administración, bajo la dirección del SEPD. Dichos Estados miembros sugieren que la flexibilidad concedida por los colegisladores debería utilizarse adecuadamente para maximizar la eficacia y la eficiencia de las funciones de Europol y garantizar su pertinencia y rentabilidad a largo plazo.

Sin embargo, una evaluación de los métodos de trabajo de Europol y de los posibles ámbitos de simplificación queda fuera del ámbito del informe con arreglo al artículo 68, apartado 3, del Reglamento Europol y se llevará a cabo en el marco de la evaluación con arreglo al artículo 68, apartado 1, de dicho Reglamento.

4. Conclusiones y perspectivas de futuro

En resumen, las principales conclusiones preliminares de la Comisión son que los Estados miembros mantienen **su apoyo a la función desempeñada por Europol** en los ámbitos clave en los que actualmente asiste a los Estados miembros en sus **nuevas funciones relativas al tratamiento de datos personales**. Sin embargo, en opinión de algunas partes interesadas, para **maximizar los beneficios** de las nuevas competencias en materia de tratamiento de datos personales será necesario **abordar posibles deficiencias**, en particular en el marco actual de gobernanza, administración y protección de datos, que pueden retrasar y limitar su uso. También sería útil mitigar la **complejidad y fragmentación** del marco jurídico, que puede disuadir a los profesionales de hacer uso de las nuevas posibilidades.

En general, la Comisión no encontró pruebas de que las nuevas normas tuvieran un **impacto negativo en los derechos fundamentales**, en particular gracias a sólidas salvaguardias de

[45] Véanse las pruebas presentadas en la sección 5 del documento de trabajo de los servicios de la Comisión que acompaña al presente informe, y en particular las observaciones de Europol y las respuestas de los Estados miembros a las preguntas 2, 4 y 5 del cuestionario breve de 2 de junio de 2025, en el anexo III del documento de trabajo de los servicios de la Comisión y en la declaración conjunta de los jefes de policía europeos sobre el futuro de Europol.

protección de datos, que también facilitan el flujo de información al aumentar la confianza de los socios. Para algunos Estados miembros, Europol adoptó un enfoque conservador, mientras que **debería hacerse un uso adecuado de la flexibilidad concedida por los colegisladores** en lo que respecta a la categorización de los interesados, la evaluación de impacto relativa a la protección de datos, la consulta previa al Supervisor Europeo de Protección de Datos y la tramitación de las solicitudes de derechos de acceso.

Sin embargo, dado el breve período de aplicación de las nuevas normas de protección de datos personales previstas en el Reglamento (UE) 2022/991, las pruebas recogidas no son concluyentes en lo relativo a todas las cuestiones.

En su **ProtectEU**, la Estrategia Europea para la Seguridad Interior[46], la Comisión anunció que propondrá una revisión ambiciosa del mandato de Europol para hacer frente a los crecientes desafíos en materia de seguridad. De conformidad con sus directrices para la mejora de la legislación[47], la Comisión inició los preparativos para la evaluación del Reglamento Europol y los métodos de trabajo de Europol, preparando así el camino para una **propuesta de la Comisión en 2026 para que la Agencia sea más operativa, tal como se establece en las orientaciones políticas**[48]. En julio de 2025, la Comisión publicó la convocatoria de datos[49] y contrató un estudio externo para apoyar la evaluación del Reglamento de Europol y la evaluación de impacto de la nueva propuesta. La evaluación del Reglamento de Europol realizada a efectos de la elaboración del presente informe tiene por objeto contribuir a dicha evaluación.

46 «ProtectEU: una Estrategia Europea para la Seguridad Interior», p. 10.

47 Véase la página https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_es.

48 Ursula von der Leyen, Orientaciones políticas para la próxima Comisión Europea 2024-2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_en.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Cooperacion-policial-nuevo-Reglamento-de-Europol-propuesta-_es.