Consejo de la Unión Europea

Bruselas, 28 de noviembre de 2025
(OR. en)

16137/25

JAI 1814
ENFOPOL 457
CRIMORG 247
IXIM 326
DATAPROTECT 319
CYBER 356
COPEN 389
FREMP 369
TELECOM 447
COMPET 1262
MI 980
CONSOM 276
DIGIT 256

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	27 de noviembre de 2025
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2025) 740 final
Asunto:	INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre la aplicación del Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo, de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea

Adjunto se remite a las delegaciones el documento COM(2025) 740 final.

Adj.: COM(2025) 740 final

COMISIÓN
EUROPEA

Bruselas, 27.11.2025
COM(2025) 740 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

sobre la aplicación del Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo, de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea

ÍNDICE

1. INTRODUCCIÓN

Los servicios de comunicaciones interpersonales se utilizan cada vez más de manera indebida para compartir material de abuso sexual de menores (en lo sucesivo «MASM») y para el embaucamiento de menores («captación de menores»). Esto ha llevado a los proveedores de determinados servicios de comunicaciones interpersonales independientes de la numeración, como los servicios de correo web y de mensajería («proveedores»), a utilizar tecnologías específicas de forma voluntaria para detectar el abuso sexual de menores (en lo sucesivo, «ASM») en línea en sus servicios y denunciarlo a las autoridades policiales y a las organizaciones que actúan en interés público contra el ASM. Estas actividades voluntarias desempeñan un papel valioso a la hora de ayudar a detectar y rescatar a las víctimas, reducir la captación de menores y la difusión de MASM en línea, así como a prevenir, detectar, investigar y enjuiciar los delitos relacionados con el ASM. Para facilitar que continúen los esfuerzos voluntarios para detectar el ASM, el Reglamento (UE) 2021/1232[1] («el Reglamento»), modificado por el Reglamento (UE) 2024/1307, de 29 de abril de 2024[2], establece una excepción temporal a los artículos 5, apartado 1, y 6, apartado 1, de la Directiva 2002/58/CE[3].

El artículo 9 del Reglamento exige un informe de aplicación de la Comisión, basado en los datos de los proveedores y los Estados miembros, y que tenga en cuenta, en particular:

a) las condiciones para el tratamiento de datos personales pertinentes y de otro tipo establecidas en el Reglamento;
b) la proporcionalidad de la excepción prevista en el Reglamento, incluida la evaluación de las estadísticas presentadas por los Estados miembros con arreglo a su artículo 8;
c) los avances tecnológicos relativos a las actividades contempladas en el Reglamento, y la medida en que estos avances mejoran la precisión y reducen el número y las tasas de errores (falsos positivos).

El presente es el segundo informe de aplicación en virtud del Reglamento, tras el primer informe adoptado el 19 de diciembre de 2023[4]. Se basa en los datos obtenidos desde entonces,

---

1 Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo, de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea (DO L 274 de 30.7.2021, p. 41, ELI: http://data.europa.eu/eli/reg/2021/1232/oj).

2 Reglamento (UE) 2024/1307 del Parlamento Europeo y del Consejo, de 29 de abril de 2024, por el que se modifica el Reglamento (UE) 2021/1232 por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea (DO L, 2024/1307, 14.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1307/oj).

3 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

4 Informe de la Comisión al Parlamento Europeo y al Consejo relativo a la aplicación del Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo, de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea [COM(2023) 797 final].

a través de la notificación por parte de los proveedores y los Estados miembros de conformidad con su artículo 3, apartado 1, letra g), inciso vii), y su artículo 8, respectivamente.

El primer informe reveló notables disparidades en cuanto a la disponibilidad de datos, los tipos de datos recogidos y también, por consiguiente, en cuanto a la comparabilidad de los datos recogidos por los proveedores y los Estados miembros. Este segundo informe muestra que esos problemas persisten. Los proveedores no utilizaron el formulario normalizado para la presentación de informes establecido en el Reglamento de Ejecución de la Comisión adoptado el 25 de noviembre de 2024[5], tal como exige el artículo 3, apartado 4, del Reglamento, alegando que solo estuvo disponible hacia el final del período de notificación. También compartieron diferentes tipos de información que no son necesariamente comparables. Muchos Estados miembros facilitaron datos con retraso y algunos solo facilitaron datos parciales o no pudieron facilitar ninguno antes de la publicación del presente informe. La Comisión inició un seguimiento para fomentar la presentación de los datos y permitir su correcta interpretación. Esto ha afectado significativamente a los plazos y a la exhaustividad del informe general. A pesar de los intentos de garantizar la coherencia y la comparabilidad de los datos, persisten las disparidades.

El presente informe tiene por objeto ofrecer una visión general basada en hechos de la aplicación del Reglamento, tomando como base los datos disponibles. El informe no contiene ninguna interpretación del Reglamento ni se pronuncia sobre la manera en que se ha interpretado y aplicado en la práctica.

2. MEDIDAS DE APLICACIÓN

2.1. Tratamiento de datos personales por parte de los proveedores [artículo 3, apartado 1, letra g), inciso vii)]

En el artículo 3, apartado 1, letra g), inciso vii), del Reglamento se establecen las condiciones para que, a más tardar el 3 de febrero de 2022 y, posteriormente, a más tardar, el 31 de enero de cada año, los proveedores que actúen acogiéndose a la excepción prevista en él publiquen y presenten a la autoridad de control competente y a la Comisión un informe sobre el tratamiento de datos personales en virtud del citado Reglamento. Google, LinkedIn, Meta, Microsoft y Yubo presentaron informes, referentes tanto a 2023 como a 2024. El presente informe abarca los datos presentados por los proveedores referentes a los años 2023 y 2024, mientras que los datos de 2021 y 2022 se tratan en el informe anterior.

2.1.1. Tipo y volumen de datos tratados

Los proveedores notificaron el tratamiento tanto de datos de contenido como de tráfico. Por lo que se refiere a los datos de contenido tratados para detectar ASM en línea, todos los

[5] Reglamento de Ejecución (UE) 2024/2916 de la Comisión, de 25 de noviembre de 2024, por el que se establece un formulario normalizado para los datos incluidos en el informe sobre el tratamiento de datos personales publicado y presentado a la autoridad de control competente y a la Comisión por los proveedores de servicios en virtud del Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo (DO L, 2024/2916, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2916/oj).

proveedores mencionaron imágenes y vídeos. Google también se refirió al tratamiento de otros tipos de medios.

En cuanto a los datos de tráfico recabados, los informes de los proveedores variaron considerablemente:

a) datos relacionados con la cuenta de usuario (Google, LinkedIn, Microsoft y Yubo), como identificador de usuario, nombre de usuario o dirección IP;
b) metadatos relacionados con contenidos (Google, LinkedIn, Microsoft y Yubo);
c) datos relacionados con una posible víctima (Google);
d) datos de operaciones de abuso (Google).

LinkedIn y Microsoft facilitaron información sobre los volúmenes de datos tratados con arreglo al Reglamento, mientras que los demás proveedores no presentaron datos a este respecto. LinkedIn informó del tratamiento de más de 24 millones de imágenes y más de 1 millón de vídeos en 2023 y de más de 22 millones de imágenes y más de 2 millones de vídeos en 2024, procedentes de la UE en ambos años. Microsoft informó del tratamiento de más de 11 700 millones y de 9 600 millones de elementos de contenido en todo el mundo en 2023 y 2024, respectivamente, sin especificar los datos relacionados con la UE.

2.1.2. Motivos para el tratamiento de conformidad con el Reglamento (UE) 2016/679

Todos los proveedores informaron sobre la base de uno o varios de los motivos específicos previstos en el Reglamento (UE) 2016/679, el Reglamento General de Protección de Datos («RGPD»)[6]: Artículo 6, apartado 1, letra d) (Google, Meta y Yubo), letra e) (LinkedIn, Microsoft, Meta y Yubo) y letra f) (Google, Meta y Yubo).

2.1.3. Motivo para las transferencias de datos personales fuera de la UE

Todos los proveedores informaron de que se basaban en mecanismos de transferencia de datos en virtud del RGPD, como las cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el artículo 46, apartado 2, letra c), del RGPD. Google, Microsoft, LinkedIn y Yubo también informaron del cumplimiento del Marco de Privacidad de Datos UE-EE. UU.

2.1.4. Número de casos detectados de ASM en línea, diferenciando entre MASM y embaucamiento de menores

Cuadro 1: Número de casos de ASM en línea detectados en 2023

Proveedor	Número de casos	Observaciones
Google	1 558 elementos de contenido	734 denuncias sobre MASM enviadas al Centro Nacional para Niños Desaparecidos y Explotados (en lo sucesivo, «NCMEC»). Se denunció a 635 cuentas de Google por haber enviado al menos un elemento de contenido de MASM.
LinkedIn	2 elementos de contenido	LinkedIn detectó 2 imágenes y 0 vídeos que constituyen MASM.

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

Meta	3,6 millones de elementos de contenido	Elementos de contenido que constituyen MASM relacionados con usuarios de la UE.
Microsoft	9 000 elementos de contenido	Más de 32 000 elementos de contenido identificados como MASM a escala mundial durante el período, de los cuales más de 9 000 procedían de la UE.
Yubo	7 720 casos	Yubo suspendió 7 720 cuentas en la UE en 2023, 2 de ellas por haber compartido MASM conocido, 938 por haber compartido MASM nuevo y 6 780 por haber embaucado o explotado sexualmente a un menor.

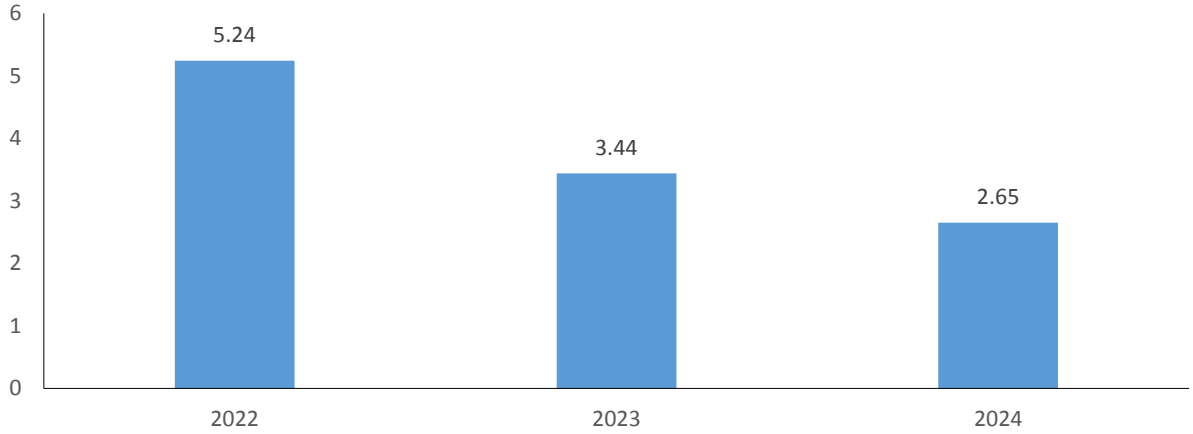
Cuadro 2: Número de casos de ASM en línea detectados en 2024

Proveedor	Número de casos	Observaciones
Google	1 824 elementos de contenido	508 denuncias de MASM enviadas al NCMEC. Se denunció a 503 cuentas de Google por haber enviado al menos un elemento de contenido de MASM.
LinkedIn	1 elemento de contenido	LinkedIn detectó 1 archivo de imagen y 0 vídeos que constituían MASM.
Meta	1,5 millones de elementos de contenido	Elementos de contenido que constituyen MASM relacionados con usuarios de la UE.
Microsoft	Más de 5 800 elementos de contenido	Más de 26 000 elementos de contenido identificados como MASM a escala mundial, de los cuales más de 5 800 procedían de la UE[7].
Yubo	4 484 casos	Yubo detectó 742 casos relativos a MASM nuevo y 3 742 casos relativos a embaucamiento de menores.

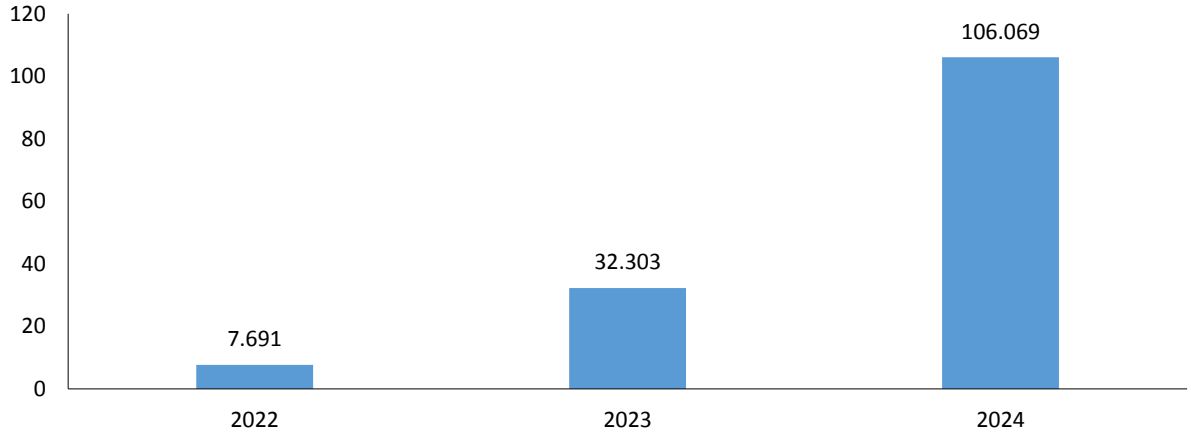
Dado que todos los proveedores mencionados informan al NCMEC en los Estados Unidos (véase la sección 2.1.9), además de otros proveedores que no han informado a la Comisión, los datos del NCMEC proporcionan, en principio, una visión más completa de las denuncias de ASM en la UE. El NCMEC informó de haber recibido anualmente el siguiente número de elementos de contenido (imágenes, vídeos y otros archivos) y de casos de embaucamiento de menores relacionados con la UE:

[7] Los datos comunicados por Microsoft revelan que la proporción entre los elementos de contenido identificados como MASM y los elementos de contenido tratados se mantuvo constante entre 2023 y 2024, en el 0,00027 %.

Número de imágenes, vídeos y otros archivos contenidos en las denuncias del NCMEC relativas a la UE (en millones)



Número de denuncias de captación de menores del NCMEC relativas a la UE (en miles)



2.1.5. Recursos de usuarios y resultado

De conformidad con el artículo 3, apartado 1, letra g), inciso iv), del Reglamento, los proveedores deben establecer procedimientos y mecanismos de recurso adecuados para garantizar que los usuarios puedan presentar reclamaciones ante ellos. Además, el artículo 5 establece normas sobre la tutela judicial.

Todos los proveedores notificaron cifras de reclamaciones de usuarios en relación con las cuestiones contempladas en el ámbito de aplicación del Reglamento dentro de la UE, así como los resultados de dichas reclamaciones. Los proveedores se refirieron a reclamaciones contra la retirada de elementos de contenido o a reclamaciones contra la suspensión de cuentas de usuario, sin presentar información separada sobre ambas categorías. Google y Yubo también informaron por separado sobre las reclamaciones presentadas ante una autoridad judicial. Por consiguiente, los cuadros que figuran a continuación reflejan los procedimientos de recurso

interno e incluyen información sobre el recurso judicial en las observaciones si los datos están disponibles. Hasta la fecha, no se ha notificado ningún caso de reclamación ante una autoridad judicial.

Cuadro 3: Número de casos en los que un usuario ha presentado una reclamación ante el mecanismo de recurso interno o ante una autoridad judicial y el resultado de dichas reclamaciones en 2023

Proveedor	Reclamaciones de usuarios	Cuentas restablecidas	Elementos de contenido restablecidos	Observaciones
Google	297	10	n/d	El número de casos de reclamaciones de usuarios refleja los recursos contra la suspensión de una cuenta de usuario presentados ante el mecanismo de recurso interno. Ningún usuario presentó una reclamación ante una autoridad judicial.
LinkedIn	0	n/d	n/d	
Meta	254 500 aprox.	n/d	11 600 aprox.	Los usuarios recurrieron las medidas adoptadas en relación con alrededor de 254 500 elementos de contenido. Tras el procedimiento de recurso, se restablecieron unos 11 600 elementos de contenido y se revirtieron las medidas tomadas respecto a las cuentas.
Microsoft	0	n/d	n/d	
Yubo	1 159	50	n/d	Yubo estima que, a raíz de estos recursos, se restablecieron aproximadamente 50 cuentas con origen en la UE. Ningún usuario presentó una reclamación ante la autoridad judicial de la UE.

Cuadro 4: Número de casos en los que un usuario ha presentado una reclamación ante el mecanismo de recurso interno o ante una autoridad judicial y el resultado de dichas reclamaciones en 2024

Proveedor	Reclamaciones de usuarios	Cuentas restablecidas	Elementos de contenido restablecidos	Observaciones
Google	216	19	n/d	El número de casos de reclamaciones de usuarios refleja los recursos contra la suspensión de una cuenta de usuario presentados ante el mecanismo de recurso interno. Ningún usuario

				presentó una reclamación ante una autoridad judicial.
LinkedIn	1	n/d	n/d	
Meta	76 900 aprox.	n/d	1 800 aprox.	Los usuarios recurrieron las medidas adoptadas en relación con alrededor de 76 900 elementos de contenido. Tras el procedimiento de recurso, se restablecieron unos 1 800 elementos de contenido y se revirtieron las medidas tomadas respecto a las cuentas.
Microsoft	0	n/d	n/d	
Yubo	31	0	n/d	Yubo recibió 31 reclamaciones contra una suspensión relacionada con la seguridad infantil en la UE. No se restableció ninguna cuenta (0).

2.1.6. Número y tasas de errores (falsos positivos) de las diferentes tecnologías utilizadas

De conformidad con el artículo 3, apartado 1, letra e), del Reglamento, los proveedores deben garantizar que las tecnologías utilizadas sean lo suficientemente fiables en cuanto que limiten en la mayor medida posible la tasa de errores en la detección de contenidos que representan ASM en línea.

A este respecto, todos los proveedores informaron de que aplicaron un enfoque por niveles para detectar ASM combinando distintas tecnologías de detección a fin de aumentar la precisión. Además, existe una compensación entre falsos positivos (es decir, cuando la herramienta señala, por ejemplo, que una imagen puede constituir MASM incorrectamente) y falsos negativos (es decir, cuando la herramienta no señaliza, por ejemplo, el ASM), ya que reducir una tasa de error suele aumentar la otra. Esta circunstancia se traduce en que el proveedor puede adaptar los parámetros de precisión para elegir el equilibrio adecuado en función del contexto y la naturaleza específicos del servicio.

Los proveedores utilizaron tecnologías de coincidencia de hashes, como PhotoDNA, MD5 y CSAI Match, para detectar coincidencias de MASM anteriormente identificado. También se informó del uso de inteligencia artificial (IA) y clasificadores de aprendizaje automático para detectar MASM nuevo (Google y Yubo). Yubo también informó de la detección de embaucamiento de menores.

Los proveedores no presentaron el número ni las tasas de errores (falsos positivos) de cada una de las distintas tecnologías utilizadas por separado. En su lugar, notificaron datos agregados de todas las tecnologías utilizadas.

Los datos presentados muestran diferentes métodos utilizados a la hora de calcular la tasa de error. Algunos proveedores no disponían de datos suficientes para calcular la tasa de error (Microsoft). Otros aplicaron un método de cálculo basado en la relación general entre los elementos de contenido restablecidos o las medidas tomadas respecto a la cuenta revertidas y los elementos de contenido objeto de medidas, o basado en el número de recursos contra las restricciones de las cuentas (Meta y LinkedIn). Otros proveedores (Google y Yubo) se refirieron al número de elementos de contenido marcados automáticamente como constitutivos

de MASM que posteriormente no se confirmaron como tal tras una revisión humana (falsos positivos) dividido entre el número de elementos de contenido señalizados automáticamente como constitutivos de MASM. Por lo tanto, los cuadros que figuran a continuación reflejan las disparidades en los conjuntos de datos presentados por los proveedores.

A fin de reducir aún más los errores y los falsos positivos, los proveedores también informaron de que complementaban el uso de estas tecnologías con revisiones humanas. Estas no se han tenido en cuenta en las estadísticas que figuran a continuación, en que solo se considera la exactitud de las propias tecnologías.

Cuadro 5: Número y tasas de error en 2023 y 2024

Proveedor	Tasa de error en 2023	Tasa de error en 2024	Método de cálculo	Observaciones
Google	1,14 % (18:1576)	0,54 % (10:1834)	Relación entre el número de elementos de contenido marcados automáticamente como MASM que no se confirman tras una revisión humana y el número de elementos de contenido señalizados automáticamente como MASM	Los datos se refieren a tecnologías de coincidencia de hashes de Google.
LinkedIn	0 % (0:0)	0 % (0:0)	Relación entre las medidas tomadas respecto a la cuenta revertidas y los recursos contra las restricciones de las cuentas	
Meta	0,32 % (11 600 frente a 3.6 millones)	0,12 % (1 800 frente a 1.5 millones)	Relación entre los elementos de contenido restablecidos y las medidas tomadas respecto a la cuenta revertidas, y los elementos de contenido objeto de medidas	
Microsoft	n/d	n/d	n/d	Microsoft indicó que los datos eran insuficientes para calcular una tasa de error. Se revocaron decisiones iniciales de moderación de contenidos relacionadas con 34 elementos de contenido. No se ha notificado ningún recurso.

Yubo	20 %	13 %	Casos señalizados automáticamente como captación de menores en que los moderadores no tomaron medidas	Los datos facilitados por Yubo se refieren únicamente a la detección de MASM nuevo y de casos de captación de menores.

2.1.7. Medidas aplicadas para limitar la tasa de error y la tasa de error alcanzada

De conformidad con el artículo 3, apartado 1, letra e), del Reglamento, las tecnologías utilizadas deben ser lo suficientemente fiables y las consecuencias de cualquier error ocasional deben rectificarse sin demora. Además, el artículo 3, apartado 1, letra g), inciso ii), exige a los proveedores que garanticen la supervisión y, en caso necesario, la intervención humanas.

Los proveedores notificaron la aplicación de diferentes medidas y salvaguardias para limitar y reducir la tasa de error en la detección de ASM en línea. Entre ellas, cabe citar las siguientes:

i. el seguimiento y la evaluación de la calidad del funcionamiento de las herramientas de detección de ASM para afinar su precisión (de forma que detecten solo el ASM en línea) y a modo de recordatorio (de que no están pasando por alto ASM en línea en sus plataformas) (Google);
ii. la aplicación de procedimientos de verificación de hashes en que los analistas revisan elementos asociados a bases de datos sobre los códigos hash o comprueban la calidad de los hashes existentes (Google, Microsoft y LinkedIn);
iii. la revisión y supervisión humanas: los medios detectados como MASM por tecnologías de coincidencia de hashes son auditadas por revisores humanos / analistas formados (Google, LinkedIn, Meta, Microsoft y Yubo);
iv. la revisión humana sistemática de los medios detectados como posibles MASM nuevos antes de la notificación (Google en 2023);
v. revisores humanos que han recibido una formación especializada o una nueva certificación periódica (Google y Yubo);
vi. las evaluaciones de control de la calidad de los revisores humanos y de los veredictos que se aplican (Google y Yubo);
vii. la elaboración y la revisión periódica de políticas y estrategias de ejecución a cargo de expertos formados en materia de ASM en línea (Google);
viii. las consultas periódicas con expertos para mejorar la precisión en la detección del MASM, con la inclusión de canales para recibir observaciones de organizaciones de confianza que luchan contra el ASM, como NCMEC y Thorn (Google);
ix. el sistema de alerta que garantiza que se señalicen y revisen agrupaciones de un volumen elevado (Meta);
x. medidas para mejorar la calidad de los algoritmos de seguridad (Yubo).

2.1.8. Política de conservación y salvaguardias de protección de datos

Las letras h) e i) del artículo 3, apartado 1, del Reglamento exigen que los datos personales pertinentes se almacenen de manera segura y únicamente con determinados fines especificados, y contienen especificaciones en cuanto al período de almacenamiento, respectivamente. Además, deben respetarse los requisitos aplicables del RGPD.

Todos los proveedores informaron de que contaban con sólidas políticas de conservación y salvaguardias de protección de datos personales en vigor. Las políticas de conservación de datos varían en función del tipo de datos. Los proveedores señalan que, en cada caso, el período de conservación está limitado en el tiempo, en función del tipo de datos y la finalidad del tratamiento, y que los datos se suprimen al final del período de conservación. La mayoría de los proveedores (Google, Meta y LinkedIn respecto a 2024) también notificaron la aplicación de una política de conservación máxima de doce meses del MASM detectado. Yubo informó de que los datos sobre moderación de contenidos suelen conservarse durante doce meses y de que los períodos de conservación dependen del tipo de contenido, el tipo de infracción y las condiciones de almacenamiento. Meta informó, en 2024, de que conservaba los datos sobre los recursos de los usuarios durante un período de 195 días.

Las salvaguardias de protección de datos notificadas por los proveedores son, entre otras:

i. el uso de técnicas de anonimización o seudonimización (por ejemplo, enmascaramiento, *hashing*, privacidad diferencial) (Microsoft);
ii. el uso del cifrado de los datos en tránsito (por ejemplo, protocolos TLS) (Meta y Yubo);
iii. los controles de acceso (Meta y Yubo);
iv. la aplicación de estrategias de gobernanza de datos o programas de privacidad, garantizando que solo se acceda a los datos, se utilicen o se compartan de manera autorizada (Google);
v. la realización de revisiones de privacidad para detectar los posibles riesgos para la privacidad derivados de la recogida, el tratamiento, el almacenamiento y el intercambio de datos personales, acceder a ellos y mitigarlos, y de revisiones de las prácticas de protección cuando se diseñan nuevas capacidades o procesos del sistema (Microsoft);
vi. la rápida investigación de los incidentes notificados por parte del equipo de respuesta (Google);
vii. las medidas sobre los mecanismos de recurso interno y la información a los usuarios, en particular las dirigidas a garantizar el derecho de acceso a los datos de los usuarios (Google en 2024).

2.1.9. Organizaciones que actúan en interés público con las que se han compartido datos

Todos los proveedores informaron de que compartían los datos en virtud del presente Reglamento con el NCMEC. Todos los proveedores que presentaron informes comunicaron asimismo a la Comisión, de conformidad con el artículo 7, apartado 1, del Reglamento, que habían denunciado al NCMEC el ASM en línea con arreglo al Reglamento[8]. Yubo también informó de la puesta en común de datos con la Internet Watch Foundation (IWF) en el Reino Unido y con PHAROS (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) en Francia.

[8] La información sobre las organizaciones que actúan en interés público a las que los proveedores denuncian el ASM en línea con arreglo al Reglamento se ha publicado en https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/legal-framework-protect-children_en?prefLang=es [en inglés], de conformidad con la obligación de la Comisión prevista en el artículo 7, apartado 2, del Reglamento.

2.2. Estadísticas de los Estados miembros (artículo 8)

De conformidad con el artículo 8, apartado 1, del Reglamento, los Estados miembros deben hacer públicos y presentar a la Comisión informes con estadísticas sobre la siguiente información:

a) el número total de denuncias de ASM en línea detectados que hayan presentado los proveedores y las organizaciones que actúan en interés público contra el ASM ante las autoridades policiales nacionales competentes, diferenciando, cuando se disponga de tal información, entre el número absoluto de casos y los casos denunciados varias veces, y también según el tipo de proveedor en cuyo servicio se detectó el ASM en línea;
b) el número de menores identificados mediante acciones con arreglo al artículo 3 del presente Reglamento, desglosado por género;
c) el número de infractores condenados.

Dado que, para la elaboración del anterior informe, algunos Estados miembros notificaron datos hasta julio de 2022 y otros de todo el año 2022, el presente informe abarca todos los años civiles 2022, 2023 y 2024 para facilitar la comparabilidad. Dicho esto, los datos comunicados por los Estados miembros varían considerablemente en términos de exhaustividad y detalle. Algunos Estados miembros no facilitaron todos los datos requeridos con respecto a cada uno de los años en cuestión (Bélgica, Estonia, Irlanda, España, Croacia, Portugal y Rumanía).

2.2.1. Número total de denuncias de ASM en línea detectados

La mayoría de los Estados miembros facilitaron estadísticas anuales sobre el número total de denuncias de ASM en línea correspondientes a los años naturales 2022, 2023 y 2024, de conformidad con el artículo 8, apartado 1, letra a), del Reglamento. Portugal no facilitó datos de ninguno de los años pertinentes, mientras que España no facilitó datos de 2023 o 2024.

Los Estados miembros facilitaron en su mayoría el número total de denuncias presentadas ante las autoridades policiales nacionales por proveedores u otras organizaciones que actúan en interés público contra el ASM. La mayoría de los Estados miembros notificaron haber recibido la mayoría o la totalidad de las denuncias del NCMEC. Los Estados miembros no indicaron el número de denuncias susceptibles de ser objeto de medidas, es decir, aptas para someterse a una investigación, pero algunos de ellos señalaron el número de casos abiertos, que es significativamente menor. Los Estados miembros, salvo Dinamarca y Finlandia, tampoco diferenciaron entre el número total de casos y los casos denunciados varias veces. Solo unos pocos Estados miembros indicaron el tipo de proveedores en cuyos servicios se detectó el ASM en línea (por ejemplo, Bélgica, Irlanda, Polonia y Rumanía). Algunos facilitaron un desglose detallado (Bélgica, Chequia, Francia, Luxemburgo, Rumanía y Finlandia).

Cuadro 6: Número total de denuncias de ASM detectados comunicadas por los Estados miembros

País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
AT	10 130	15 882	18 276	NCMEC[9]	
BE	19 919	11 910	4 284	Denuncias procedentes de proveedores (redes sociales)	El número de proveedores que detectaron ASM en línea aumentó entre 2022 y 2024. Respecto a 2024, Bélgica solo notificó el número de denuncias susceptibles de ser objeto de medidas, cambiando la metodología utilizada en años anteriores.
BG	25 303	38 026	71 187	NCMEC e INHOPE (*International Association of Internet Hotlines*)	Durante los tres años en cuestión, se recibieron 42 596 denuncias del NCMEC y 92 010 de Safenet.
CY	2 809	3 516	5 380	NCMEC	
CZ	23 854	21 658	22 580	NCMEC, CZ.NIC (Asociación Checa de Proveedores de Servicios de Internet)	En 2024 se recibieron denuncias de 57 proveedores de servicios diferentes, siendo Instagram el primero (11 857 denuncias), seguido de Facebook (4 461), Snapchat (3 610), Imgur (1 705), Discord (1 510), Google (1 439), Microsoft (operaciones en línea) (870), Tik Tok (825) y WhatsApp (620).
DE	136 437	180 287	205 728	NCMEC	Alemania informó de que no podía proporcionar estadísticas propias de conformidad con el artículo 8, apartado 1, del Reglamento, alegando que no existe base jurídica para la detección voluntaria. Proporcionó estadísticas policiales sobre

[9] Todos los datos de este cuadro, incluidos los casos en que se mencionan el NCMEC u otras fuentes externas, se reproducen según lo comunicado a la Comisión por los Estados miembros.

País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
					delincuencia, destacando que el año en el que se cometió el delito no coincide necesariamente con el año de aparición en las estadísticas: en cuanto al abuso sexual de niños y jóvenes, hubo 16 655 casos en 2022 y 17 575 en 2023 (+ 6 %); en cuanto a la difusión, adquisición y posesión de material de abuso sexual de niños y jóvenes, hubo 48 853 casos en 2022 y 54 042 casos en 2023 (+ 11 %).
DK	7 556	9 938	10 918	NCMEC	En 2022 se iniciaron 2 474 casos, 2 278 en 2023 y 2 097 en 2024. 90 de los casos abiertos se basaron en MASM notificado varias veces en años diferentes.
EE	250	305	274	NCMEC, Línea telefónica de ayuda a la infancia: 116 111	Estonia informó de que las estadísticas de su policía y su guardia de fronteras, entre ellas los datos del NCMEC, no son públicas. En 2022 se denunciaron 250 delitos sexuales contra menores sin contacto y, en 2023, 305. El 88 % de todos los delitos sexuales sin contacto de 2022 se cometieron en el entorno en línea. Los datos disponibles para 2024 corresponden a casos registrados por la policía y hechos públicos en la encuesta sobre delincuencia realizada por el Ministerio de Justicia y Asuntos Digitales. Estas estadísticas proceden del NCMEC y no son estadísticas nacionales.

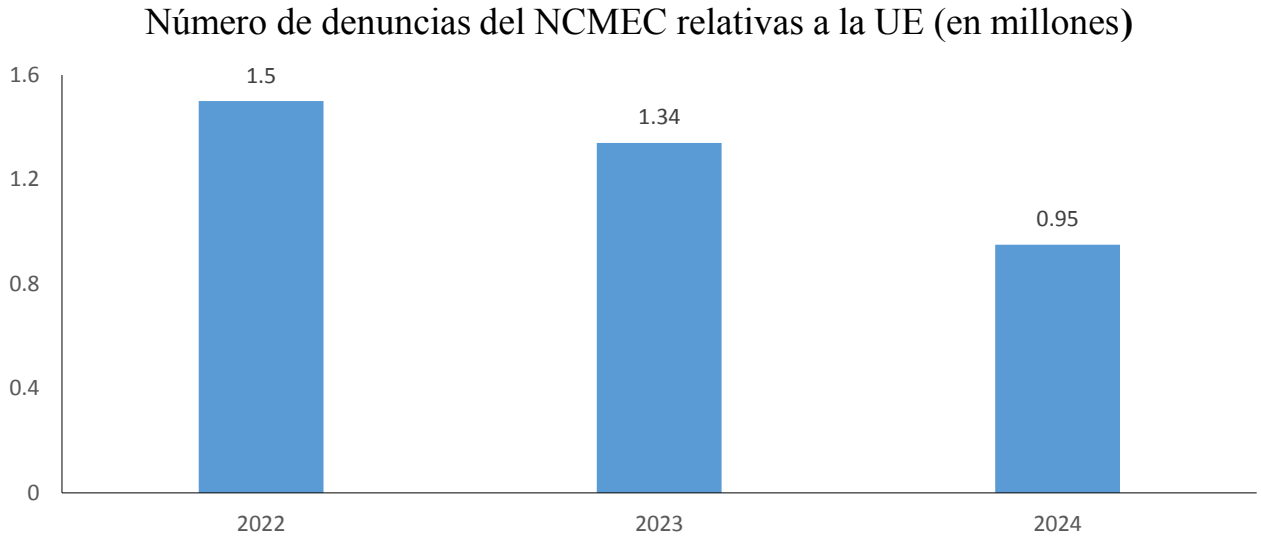
País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
EL	121	103	123	NCMEC, línea directa griega para contenidos ilegales en internet (Safeline), Interpol, Europol y The Smile of the Child (organización griega sin ánimo de lucro)	
ES	31 474	-	-	Organizaciones que actúan en interés público contra el ASM	Datos de 2023 o 2024 no presentados.
FI	11 248	16 781	13 954	NCMEC y otros canales	Con respecto a los datos de 2024, el número exacto de casos notificados varias veces no puede deducirse de las bases de datos, pero el NCMEC estima que el número de estas denuncias duplicadas se sitúa entre 20 y 300. Parece que las denuncias duplicadas son más comunes en el caso de Snapchat. Además de los datos del NCMEC, Save the Children (Finlandia) notificó 71 dominios y 439 URL, la iniciativa nacional Sua varten somessa [«Para ti en las redes sociales»] notificó 90 incidentes, y otras organizaciones y proveedores notificaron menos de 10 incidentes.
FR	227 645	335 408	164 516	NCMEC, NCECC (Centro Nacional de Delitos de Explotación Infantil de Canadá), oficinas centrales nacionales de Interpol, aplicación de la red de intercambio seguro de información de Europol (SIENA), plataforma del Ministerio del Interior (PHAROS)	En 2024 se recibió un total de 158 503 denuncias del NCMEC, de las cuales 28 737 estaban relacionadas con la sextorsión de menores por motivos económicos y la corrupción de menores.
HR	11 693	8 010	8 900	Proveedor de servicios de internet	

País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
HU	109 477	25 720	25 092	Proveedores y organizaciones que actúan en interés público contra el ASM	No se dispone de información sobre los casos denunciados varias veces ni sobre los servicios en los que se detectó el material.
IE	9 168	10 785	13 334	NCMEC	Las autoridades no registran imágenes o vídeos denunciados varias veces.
IT	4 607	7 389	9 001	Asociaciones y proveedores	Dado que todavía no se han procesado todos los datos de 2024, las cifras no son definitivas.
LT	4 992	6 353	6 803	No especificado	
LU	789	1 641	2 112	NCMEC y BeeSecure (Centro de Seguridad en Internet de Luxemburgo)	Se presentaron datos sobre el desglose de las denuncias del NCMEC y BeeSecure correspondientes a 2023 y 2024, pero no están claros, ya que el número de denuncias de los proveedores no coincide con el total indicado.
LV	6	29	30	NCMEC, GRID COP, ICACCOPS (Sistema de Protección Infantil en Línea frente a Delitos Informáticos contra Menores), Centro de Seguridad en Internet de Letonia	El número total de denuncias presentadas no incluye aquellas en que el proceso penal no se inició tras la verificación, ya que no constan contabilizadas por separado. Solo una parte de las denuncias contiene indicios de que el delito está relacionado con Letonia.
MT	840	1 943	272	Línea directa nacional (Childwebalert.gov.mt), red europea de Centros de Seguridad en Internet y líneas directas gestionadas por INSAFE e INHOPE (BeSmartOnline)	
NL	36 536	70 057	70 351	Proveedores y organizaciones que actúan en interés público contra el ASM	

País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
PL	145	117	9 293	Proveedores y organizaciones que actúan en interés público contra el ASM, uno de los cuales es Dyżurnet.pl	
PT	-	-	-	-	Datos no presentados.
RO	5 705	1 254	13 384	Save the Children	El número de denuncias de ASM en línea, según Rumanía, se refiere a ASM alojados por proveedores rumanos, pero la mayoría de los clientes no procedían de Rumanía.
SE	16 800	22 592	23 834	NCMEC	El número total de denuncias recibidas no es el mismo que el número real de denuncias policiales que deben investigarse, ya que una denuncia policial puede corresponder a varias denuncias de proveedores sobre el mismo usuario y porque no todas las denuncias reflejan delitos con arreglo al Derecho penal sueco. El número de denuncias policiales es considerablemente mayor en 2023 que en 2022 y 2024. Esto se debe a que en 2023 se llevó a cabo una operación nacional destinada a gestionar todas las denuncias del NCMEC no prioritarias desde 2018.
SI	165	203	251	Proveedores y organizaciones que actúan en interés público contra el ASM	Los datos estadísticos disponibles no permiten a Eslovenia separar los datos estadísticos sobre las infracciones investigadas a partir de denuncias presentadas por proveedores y organizaciones, de los datos estadísticos referentes a otras denuncias. No se dispone de datos sobre el número absoluto

País	Denuncias en 2022	Denuncias en 2023	Denuncias en 2024	Fuente de las denuncias	Observaciones
					de casos, sobre los casos notificados varias veces o desglosados por tipo de proveedor en cuyo servicio se detectó el ASM en línea. Además, la infracción penal de agresión sexual a una persona menor de 15 años con arreglo al artículo 173 del Código Penal no se incluyó en las estadísticas facilitadas, ya que en la mayoría de los casos este delito se produce en el entorno físico, aunque en menor medida también de forma virtual.
SK	7 628	9 601	9 017	Proveedores y organizaciones que actúan en interés público contra el ASM	No se dispone de información sobre los casos notificados varias veces.
Total	**705 297**	**799 508**	**708 894**		

Dado que el NCMEC es la principal fuente de denuncias, es esclarecedor observar las cifras de las denuncias relativas a los Estados miembros que el NCMEC recibió y remitió a estos[10]:



El desglose por Estado miembro del número total de denuncias es el siguiente:

Cuadro 7: Denuncias del NCMEC de ASM en línea relativas a los Estados miembros de la UE en 2022, 2023 y 2024

País	Denuncias totales en 2022[11]	Denuncias totales en 2023[12]	Denuncias totales en 2024[13]
Austria	18 501	19 630	17 425
Bélgica	50 255	41 926	26 752
Bulgaria	31 937	17 726	30 684
Croacia	11 693	16 339	8 821
Chipre	7 361	7 564	5 750
Chequia	61 994	34 342	21 589
Dinamarca	30 215	12 048	10 330
Estonia	6 408	4 338	4 540
Finlandia	10 904	16 364	12 779
Francia	227 465	310 519	150 684
Alemania	138 193	173 560	197 201
Grecia	43 345	24 985	16 737

[10] El gráfico contiene el número total de denuncias recibidas por la UE desduplicadas, es decir, contabilizadas una sola vez si la misma denuncia se envió a varios Estados miembros.

[11] NCMEC, Informes por país de la CyberTipline de 2022, 2022, consultados el 26 de mayo de 2025.

[12] NCMEC, Informes por país de la CyberTipline de 2023, 2023, consultados el 26 de mayo de 2025.

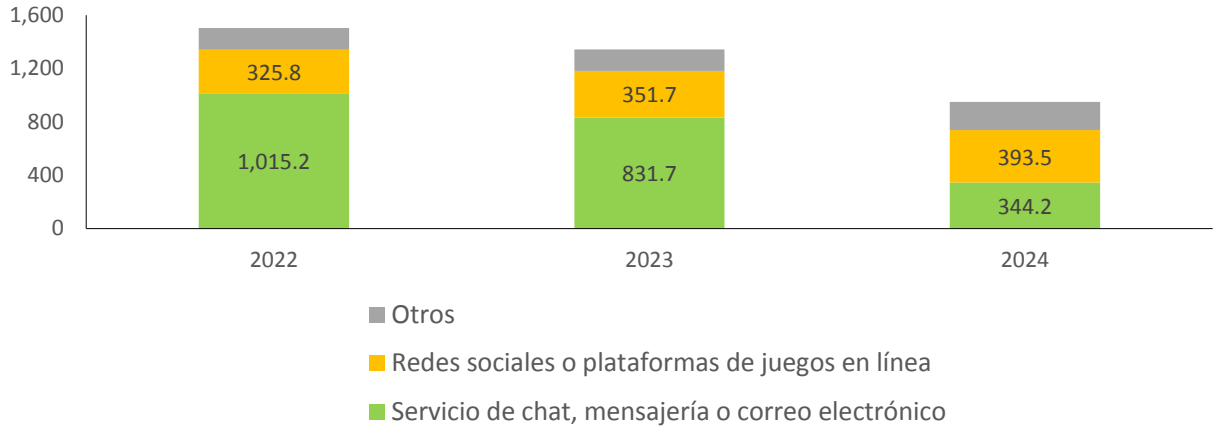
[13] NCMEC. En 2024, el NCMEC empezó a informar en su sitio web (Informes por país de la CyberTipline de 2024) del número total de denuncias enviadas a cada país. La misma denuncia se envía a varios países, si afecta a todos ellos. Los datos comunicados en el cuadro 7 de 2022, 2023 y 2024 son denuncias desduplicadas, es decir, la misma denuncia solo se cuenta una vez.

País	Denuncias totales en 2022[11]	Denuncias totales en 2023[12]	Denuncias totales en 2024[13]
Hungría	109 434	25 643	16 718
Irlanda	19 770	13 265	13 604
Italia	96 512	90 424	75 274
Letonia	3 688	4 671	6 618
Lituania	16 603	12 005	7 682
Luxemburgo	2 004	3 000	2 115
Malta	4 713	1 713	1 233
Países Bajos	57 012	72 913	68 611
Polonia	235 310	108 800	79 174
Portugal	42 674	45 675	24 707
Rumanía	96 287	133 054	44 424
Eslovaquia	39 748	13 164	8 647
Eslovenia	14 795	6 204	4 685
España	77 727	104 748	68 733
Suecia	48 883	29 237	25 300
Total	**1 503 431**	**1 343 857**	**950 817**

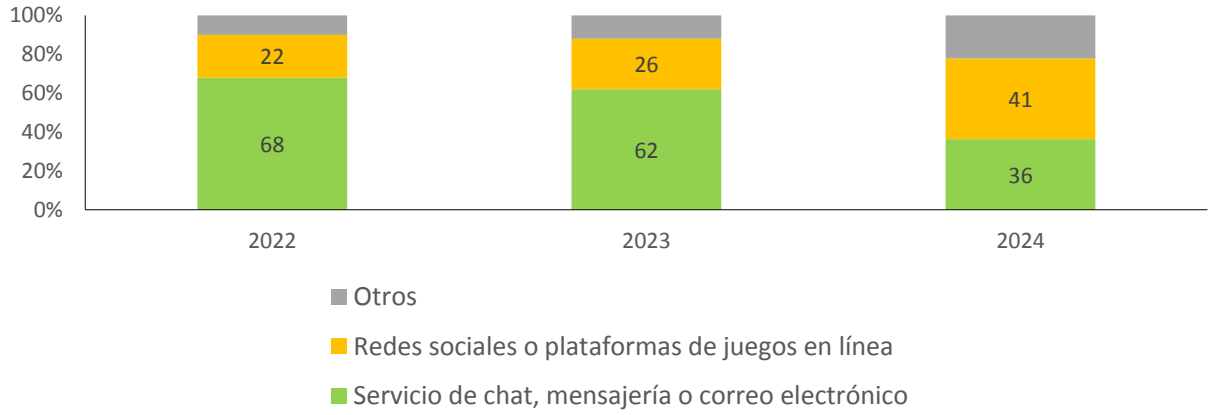
La notable disparidad entre el número de denuncias que el NCMEC declara haber remitido a cada Estado miembro y el número de denuncias que estos declaran haber recibido indica que la recogida y notificación de datos por parte de los Estados miembros no es exhaustiva.

Las estadísticas del NCMEC por Estado miembro no distinguen entre la fuente de la denuncia, en particular si esta procedía de un servicio de comunicaciones interpersonales independiente de la numeración. No obstante, el NCMEC sí proporciona estadísticas sobre el número total de denuncias que incumben a la UE procedentes de servicios de comunicaciones interpersonales independientes de la numeración, como chats, servicios de mensajería o de correo electrónico. El NCMEC también compartió cifras sobre denuncias procedentes de redes sociales o plataformas de juegos en línea, con inclusión de sus servicios integrados de mensajería o chat.

Denuncias del NCMEC relativas a la UE, por tipo de servicio en línea (en miles)



Denuncias del NCMEC relativas a la UE: tipo de servicio en línea (en %)



En 2024 se produjo un descenso significativo (30 %) en el número de denuncias relativas a la UE. Esto refleja una tendencia mundial, ya que las denuncias alcanzaron los 31,9 millones en 2022 y los 35,93 millones en 2023, para caer a 19,85 millones en 2024. El NCMEC atribuye esta caída en parte a una reducción de las denuncias de los servicios de mensajería interpersonal, ya que dichos servicios están pasando a utilizar el cifrado de extremo a extremo y los proveedores detienen los intentos de detección[14]. La caída en la proporción de denuncias procedentes de servicios de mensajería interpersonal parece indicar, en efecto, que una gran parte de la reducción puede atribuirse a una menor notificación por parte de dichos servicios.

[14] *Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary*, 11 de marzo de 2025.

2.2.2. Número de menores identificados

La mayoría de los Estados miembros facilitaron estadísticas sobre el número de menores identificados, de conformidad con el artículo 8, apartado 1, letra b), del Reglamento. Tres Estados miembros no facilitaron datos (Bélgica, Portugal y Rumanía), mientras que otros solo facilitaron datos de determinados años (por ejemplo, Finlandia de 2023 y 2024 y España de 2022). Muchos Estados miembros no pudieron desglosar por género.

Varios Estados miembros solo notificaron estadísticas parciales, señalando, por ejemplo, que los datos no están disponibles porque no forman parte de la recogida de datos estadísticos nacionales, que las autoridades nacionales no registran estas estadísticas (Bélgica, Francia y Finlandia) o que la recogida de datos estadísticos nacionales no contempla el desglose por géneros (Chequia, Chipre, Lituania, Hungría, y los Países Bajos). En muchos Estados miembros, en los datos que figuran a continuación no se distingue entre menores víctimas de ASM en línea y fuera de línea, por lo que es posible que los datos no se correspondan con el número real de casos de ASM en línea (por ejemplo, Alemania, Chipre y Luxemburgo). Por lo tanto, los datos incluyen tanto a las víctimas identificadas sobre la base de una denuncia de un proveedor como los casos en que, por ejemplo, las propias víctimas o un tercero pueden haber denunciado la infracción penal (por ejemplo, Alemania y Luxemburgo). En otros casos, el número de menores víctimas de ASM identificados solo se refiere a los ciudadanos de ese país o a las personas que residen en él, de manera que se excluye a los menores de otras nacionalidades y a los menores no identificados (por ejemplo, Letonia y Lituania).

Cuadro 8: Número de menores identificados, desglosado por género

País	2022		2023		2024		Observaciones
	Género femenino (F)/ masculino (M)/ no identificado	Total	F/M/Género no identificado	Total	F/M/Género no identificado	Total	
AT	4/2	6	9/4	13	3/3	6	Número de niños identificados sobre la base de las denuncias del NCMEC.
BE	-	-	-	-	-	-	Datos no disponibles.
BG	50/12	62	25/27	52	32/28	60	
CY	-	102	-	106	-	131	Datos desglosados por género no disponibles. Las cifras totales se refieren a las víctimas de todos los casos de explotación sexual de menores investigados.
CZ	-	45	-	53	5/15	20	Solo se dispone de datos desglosados por género para 2024. Los niños contabilizados en 2024 son víctimas de sextorsión.
DE	-	18 379	14 979/ 4795	19 774	-	19 344	Dado que las estadísticas no desglosan los motivos o los orígenes de las investigaciones, los datos pueden contener casos detectados únicamente debido a una denuncia de un proveedor y casos no relacionados en modo alguno con internet.

País	2022		2023		2024		Observaciones
	Género femenino (F)/ masculino (M)/ no identificado	Total	F/M/Género no identificado	Total	F/M/Género no identificado	Total	
DK	62/70	132	22/35	57	62/43	105	Las estadísticas se basan en las cifras del sistema de gestión de casos policiales (POLSAS) y no son definitivas, ya que algunos casos siguen pendientes. Además, los menores identificados por otros medios, incluso en casos anteriores o en un contexto internacional, no están representados en las estadísticas.
EE	24/23	47	22/29	51	19/14	33	
EL	9/0	9	26/1	27	14/0	14	
ES	80/39	119	-	-	-	-	No se han presentado los datos de 2023 y 2024.
FI	-	No disponible	-	526	-	1 045	Es probable que el número de víctimas menores de edad sea mayor, ya que señalizar el caso como ASM en línea requiere un trabajo manual de clasificación.
FR	-	n/d	-	5	-	60	
HR	4/0	4	6/0	6	6/17	23	
HU	-	30	-	12	-	200	Datos desglosados por género no disponibles.
IE	25/26	51	50/65	115	20/53	73	

País	2022		2023		2024		Observaciones
	Género femenino (F)/ masculino (M)/ no identificado	Total	F/M/Género no identificado	Total	F/M/Género no identificado	Total	
IT	-	385	-	434	-	500	Los casos identificados de sextorsión fueron los siguientes: 21 F y 111 M en 2022; 20 F y 117 M en 2023; 21 F y 109 M en 2024. Se tuvieron en cuenta los casos de captación de menores: 75 F y 46 M en 2022; 81 F y 82 M en 2023; 124 F y 11 M en 2024.
LT	-	10	-	25	-	21	Las cifras se refieren a los menores identificados como víctimas que son ciudadanos de Lituania o residen en este país. La mayoría de las investigaciones se refieren a menores no identificados, principalmente en relación con material producido en un país extranjero.
LU	-	0	3/0	3	1/0	1	Las cifras no están necesariamente vinculadas a la detección en línea.
LV	-	0	5/1	6	8/0	8	Las cifras se refieren únicamente a los niños que residen en Letonia.

País	2022		2023		2024		Observaciones
	Género femenino (F)/ masculino (M)/ no identificado	Total	F/M/Género no identificado	Total	F/M/Género no identificado	Total	
MT	2/4	6	408/470/11	889	9/9	18	Los datos de 2023 se refieren a niños identificados por la Fundación de Servicios de Bienestar Social (FSWS), mientras que los datos de 2022 y 2024 se refieren a estadísticas policiales.
NL	-	n/d	-	676	-	359	Datos desglosados por género no disponibles.
PL	520/82/23	566	133/34/140	307	109/25	134	
PT	-	-	-	-	-	-	Datos no presentados.
RO	-	-	-	-	-	-	Datos no presentados. No se han identificado víctimas rumanas ni materiales producidos en Rumanía, lo que este país atribuye a que la mayoría de los materiales ya eran conocidos internacionalmente.

País	2022		2023		2024		Observaciones
	Género femenino (F)/ masculino (M)/ no identificado	Total	F/M/Género no identificado	Total	F/M/Género no identificado	Total	
SE	3/0	3	16/10/2	28	53/65	118	Los menores identificados en casos que no dieron lugar a denuncias policiales se han excluido de las estadísticas. En algunos casos, incluso si se identificó a la víctima, la investigación no dio lugar necesariamente a una condena. El número de niños identificados a través de registros de chats se han incluido en las estadísticas.
SI	83/15	98	121/38	159	161/30	191	Los datos estadísticos se han obtenido de la base de datos actual y están sujetos a cambios.
SK	11/6	17	3/2	5	7/2	9	
TOTAL		**20 071**		**23 329**		**22 473**	

Dado que la mayoría de los Estados miembros notificaron cifras parciales de los períodos en cuestión o no pudieron diferenciar en función de si la detección voluntaria era el origen de la investigación, y que algunos no presentaron datos, no es posible calcular el número total de menores identificados como víctimas sobre la base de las denuncias de ASM en línea en la UE. No obstante, de los datos y de la información facilitada por los Estados miembros puede inferirse que se ha identificado un número de víctimas significativo gracias a una denuncia voluntaria de conformidad con el Reglamento.

2.2.3. Número de infractores condenados

Si bien la mayoría de los Estados miembros cumplieron su obligación de facilitar estadísticas sobre el número de infractores condenados, tres no facilitaron ningún dato de conformidad con el artículo 8, apartado 1, letra c), del Reglamento (Bélgica, España y Chipre). Varios Estados miembros no facilitaron estadísticas de al menos uno de los años en cuestión de conformidad con el artículo 8, apartado 1, letra c), principalmente porque no disponían de datos (Bélgica, Alemania, Irlanda, España, Francia, Chipre, Malta, Portugal y Finlandia).

La mayoría de los Estados miembros comunicaron datos fragmentados e incompletos sobre el número de infractores condenados y utilizaron diferentes criterios para registrar la información pertinente, como se muestra en el cuadro que figura a continuación.

Cuadro 9: Número de infractores condenados

País	Número de condenas en 2022	Número de condenas en 2023	Número de condenas en 2024	Observaciones
AT	768	323	334	
BE	-	-	-	Debido a problemas técnicos, los datos no están disponibles hasta finales de 2025.
BG	17	52	60	
CY	No hubo condenas	Datos no disponibles	Datos no disponibles	No se dispone de estadísticas, ya que a los agentes de policía no siempre se les informa de los resultados de los asuntos judiciales.
CZ	33	25	12	
DE	1 847	1 779	Datos no disponibles	El Gobierno federal alemán indicó que no disponía de datos sobre procedimientos penales, ya que estos datos fueron recogidos únicamente en los 16 Estados federados por fiscales y tribunales y solo se entregaron a la Oficina Federal de Estadística alemana (*Statistisches Bundesamt* o StBA). El Gobierno federal alemán encontró cifras correspondientes a 2022 y 2023 en el sitio web de la StBA que aquí notifica.
DK	318	175	44	Las estadísticas se basan en cifras del POLSAS y no son definitivas, ya que algunos casos siguen pendientes. También están sujetos a una serie de salvedades basadas en las especificidades de la recogida de datos nacionales.
EE	1	13	4	Las cifras incluyen únicamente condenas derivadas de denuncias del NCMEC, facilitadas por Google, Dropbox, Facebook Messenger, Instagram Messenger, KIK Messenger, Snapchat y Twitch.
EL	10	13	18	
IE	Datos no disponibles	80	72	Las cifras correspondientes a los infractores condenados siguen siendo objeto de revisión. Los datos presentados se refieren a los cargos y las citaciones por año civil.
ES	Datos no disponibles	-	-	Datos no presentados.
FI	Datos no disponibles	3 621	Datos no disponibles	Las estadísticas facilitadas de 2023 se refieren al número total de condenas por todos los delitos relacionados con el ASM (es decir, tanto

País	Número de condenas en 2022	Número de condenas en 2023	Número de condenas en 2024	Observaciones
				en línea como fuera de línea). En 2023 entró en vigor una nueva legislación sobre delitos sexuales, pero las estadísticas también contienen el número de personas condenadas en virtud del antiguo Código Penal en 2023.
FR	1 124	1 223	Datos no disponibles	
HR	157	146	155	
HU	8	16	12	
IT	627	668	395	Los datos están subestimados, debido a la falta de referencias completas de los órganos jurisdiccionales. Los datos de 2024 se refieren a condenas por un conjunto reducido de delitos en comparación con los datos de 2022 y 2023.
LT	3	6	2	
LU	11	20	21	Las estadísticas no hacen distinción entre los delitos cometidos en línea y fuera de línea. Además, las condenas registradas de los años facilitados pueden vincularse a los informes realizados en los años anteriores.
LV	1	12	15	Los datos desglosados por géneros son los siguientes: 1 niño en 2022; 1 niña y 11 niños en 2023; 15 niños en 2024.
MT	-	-	-	Datos anuales no disponibles.
NL	190	240	240	Las cifras son indicativas, están redondeadas a la decena más cercana y las cifras más recientes son preliminares.
PL	194	144	125	
PT	3	3	Datos no disponibles	
RO	690	804	715	
SE	123	95	14	El número solo se refiere a las condenas relacionadas con denuncias del NCMEC y tras sentencias firmes.
SI	19	22	26	

País	Número de condenas en 2022	Número de condenas en 2023	Número de condenas en 2024	Observaciones
SK	137	118	125	Las estadísticas de 2024 no son definitivas. Los datos de 2022 y 2023 no distinguen entre el número de condenas derivadas de denuncias del NCMEC y las derivadas de otras denuncias, ni entre delitos cometidos en línea y fuera de línea.

Es importante señalar que el número de condenas no es igual al número de infractores condenados, ya que una misma persona puede ser condenada por uno o varios delitos de ASM en línea. Igualmente, las estadísticas sobre condenas notificadas para un determinado período no están necesariamente vinculadas a las denuncias recibidas en ese período (por ejemplo, Estonia y Luxemburgo). En algunos casos, no se recopilaron estadísticas sobre si las denuncias de ASM en línea (p. ej., a través del NCMEC) dieron lugar a condenas o si las condenas fueron consecuencia de la información facilitada por un proveedor o una organización pública. Solo Estonia y Suecia confirmaron de forma explícita que las estadísticas reflejan únicamente las condenas resultantes de denuncias del NCMEC. Muchos Estados miembros informaron de que las cifras no eran definitivas, ya que las investigaciones seguían en curso o los casos seguían pendientes o eran objeto de recursos (Bulgaria, Dinamarca, Italia, Países Bajos y Eslovaquia). En algunos casos, los datos comunicados por los Estados miembros no distinguen entre delitos cometidos en línea y fuera de línea (Luxemburgo, Eslovaquia, Finlandia, y Suecia).

La forma en que se recopilan los datos estadísticos a nivel nacional no permite extraer una visión global del número de infractores condenados por ASM en línea en la UE. Tampoco es posible actualmente, sobre la base de los datos disponibles, establecer un vínculo claro entre estas condenas y los informes presentados por los proveedores y las organizaciones que actúan en interés público contra el ASM en determinados períodos de notificación.

2.3. Avances tecnológicos

Las tecnologías utilizadas actualmente para detectar ASM en línea incluyen tecnologías y herramientas para detectar MASM conocido (es decir, material confirmado previamente como MASM), MASM nuevo (es decir, material distinto del MASM conocido) y embaucamiento de menores (también conocido como «captación de menores»).

La lista no exhaustiva de ejemplos que figura a continuación incluye algunas de las herramientas más utilizadas. Muchas de estas se ponen a disposición de los proveedores, las autoridades policiales y otras organizaciones que pueden demostrar un interés legítimo. Estas herramientas suelen combinarse con revisiones humanas para mejorar su precisión.

2.3.1. Detección de MASM conocido

Las tecnologías disponibles para detectar el MASM conocido se sustentan únicamente en el análisis automático de contenidos[15] y suelen basarse en el *hashing*. La tecnología de funciones de resumen (*hashing*) es un tipo de toma de huellas digitales. Crea una firma digital única (un «hash») de una imagen que, a continuación, se compara con las firmas (hashes) de otras fotografías para localizar copias de la misma imagen. Esta tecnología solo detecta hashes coincidentes y no «ve»

[15] Los proveedores no consideran que los metadatos sean una herramienta eficaz para detectar MASM. Véase, por ejemplo, Pfefferkorn R.: «Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers» [«Técnicas de confianza y seguridad independientes del contenido: resultados de una encuesta a los proveedores de servicios en línea», disponible en inglés], *Journal of Online Trust and Safety*, vol. 1, n.º 2, Stanford Internet Observatory, 28 de febrero de 2022.

ningún material que no se corresponda con el hash en cuestión. Esos valores resumen no son reversibles y, por tanto, no pueden usarse para recrear una imagen.

Existen muchas variaciones y aplicaciones de la tecnología de *hashing*, incluido el *hashing* criptográfico para detectar coincidencias exactas, y el *hashing* perceptual para detectar contenido visualmente similar incluso con pequeñas modificaciones (por ejemplo, imágenes cortadas, ajustadas o con un filtro)[16]. Entre las herramientas que se ha señalado que se utilizan para detectar MASM conocido se incluyen las siguientes: i) Microsoft PhotoDNA[17]; ii) CSAI Match de Google[18]; iii) Apple NeuralHash; iv) PDQ y TMK+PDQF[19]; v) MD5 Hash Matching; y vi) Safer (Thorn)[20].

La herramienta más utilizada es Microsoft PhotoDNA, que lleva más de quince años en uso. El porcentaje de falsos positivos se estima, sobre la base de las pruebas, en un máximo de 1 000 entre 50 000 millones[21]. Mientras que la versión original de PhotoDNA detecta MASM conocido en imágenes, también está disponible una versión para detectarlo en vídeos[22].

La tecnología se está mejorando continuamente. En mayo de 2023, Microsoft anunció la introducción de nuevas capacidades de correspondencia que permiten búsquedas más rápidas (unas 350 veces más veloces), al tiempo que reducen el coste del proceso de correspondencia sin perder precisión. Según Microsoft, la nueva biblioteca también permite una detección más exhaustiva de imágenes volteadas o giradas.

2.3.2. Detección de MASM nuevo

Las tecnologías utilizadas actualmente para detectar MASM nuevo incluyen clasificadores e IA. Un clasificador es un algoritmo que organiza los datos por clases o categorías de información etiquetadas a través del reconocimiento de patrones. Algunos ejemplos de clasificadores son los que pueden detectar la desnudez, las formas o los colores. Los clasificadores necesitan datos para su aprendizaje, y su precisión mejora a medida que se les alimenta con más datos.

---

16 Tech Coalition, *Annual Report 2024*, 2024, p. 28.

17 Microsoft, PhotoDNA | Microsoft, consultado el 26 de mayo de 2025. Véase también Microsoft, *How PhotoDNA for Video is being used to fight online child exploitation — On the Issues*, 12 de septiembre de 2018, consultado el 26 de mayo de 2025.

18 Google, *Discover our child safety toolkit*, consultado el 26 de mayo de 2025.

19 Meta, *Open sourcing foto- and video-matching Technology to Make the Internet Safer*, 1 de agosto de 2019, consultado el 26 de mayo de 2025. Véase también Medium, *Image Similarity: PDQ algorithm for real-time similarity comparison against image store | by Darwinium | Medium*, 4 de julio de 2022, consultado el 26 de mayo de 2025.

20 Safer, *Power trust and safety with purpose-built solutions*, consultado el 26 de mayo de 2025.

21 Farid H., *House Committee on Energy and Commerce, Fostering a healthier Internet to protect consumers, Testimony*, 16 de octubre de 2019.

22 Microsoft, *How PhotoDNA for video is being used to fight online child exploitation*, 12 de septiembre de 2018, consultado el 26 de mayo de 2025.

Entre las herramientas para detectar MASM nuevo cabe citar las siguientes: i) Safer Predict (Thorn)[23]; ii) API Content Safety de Google[24], y iii) la tecnología de IA de Facebook[25].

Para la detección de MASM nuevo, la tasa de exactitud (definida en términos de prevención de falsos positivos) puede fijarse muy por encima del 90 %. Por ejemplo, Thorn señala que su clasificador de MASM puede configurarse con un índice de precisión del 99 % (tanto para el MASM conocido como el nuevo), lo que implica una tasa de falsos positivos del 0,1 %[26]. Es probable que estos parámetros —y la correspondiente tasa de falsos negativos— mejoren con el aumento del uso y la retroalimentación.

Las capacidades de la industria para detectar MASM nuevo se están ampliando: un ejemplo es la nueva herramienta de detección de MASM desarrollada por Discord utilizando CLIP (un algoritmo de código abierto creado originalmente por OpenAI), entrenada para asociar imágenes y texto, lo que permite a la herramienta comprender las relaciones semánticas entre ellas. Aplicando este método a la detección de MASM, la herramienta pudo detectar MASM conocido y desconocido con resultados positivos. Discord hizo que esta tecnología fuera de código abierto para compartir la innovación con otras empresas de forma gratuita y contribuir a ampliar la lucha contra el MASM en línea[27].

2.3.3. Detección de embaucamiento de menores

Para detectar la captación de menores a tiempo, antes de que el menor comparta MASM, a diferencia de lo que ocurre con el intercambio de imágenes o vídeos, las herramientas basadas en texto son especialmente pertinentes. Las herramientas para detectar la captación de menores en las comunicaciones basadas en textos detectan patrones que apuntan a la captación de menores, sin poder deducir la sustancia del contenido. Una serie de características de las conversaciones sospechosas se califica y a estas últimas se les asigna una calificación de probabilidad global, que indica la probabilidad estimada de que la conversación implique la captación de menores. Estas calificaciones pueden servir para señalizar conversaciones para una revisión humana adicional. Al igual que en el caso de la detección de MASM, la empresa puede decidir en qué nivel fija el umbral de probabilidad, con las mismas consecuencias descritas anteriormente en lo que respecta a los falsos positivos o negativos: un umbral de probabilidad más alto significa que se señalizan para revisión menos casos que no constituyen captación de menores, pero también que pueden perderse más casos de captación de menores.

---

23 Thorn, 'Introducing Safer Predict: *using the power of AI to detect Child Sexual Abuse and Exploitation Online*, 19 de julio de 2024, consultado el 26 de mayo de 2025.

24 Google, *Fighting child sexual abuse online*, consultado el 26 de mayo de 2025.

25 Véase aquí y aquí más información sobre la herramienta de Facebook para detectar proactivamente la desnudez infantil y contenido relacionado con la explotación infantil previamente desconocido utilizando la inteligencia artificial y el aprendizaje automático.

26 Thorn, *Thorn's Automated Tool to Remove Child Abuse Content at Scale Expands to More Platforms through AWS Marketplace*, 24 de mayo de 2021.

27 Tech Coalition, *Annual Report 2024*, 2024, p. 28.

Entre las herramientas utilizadas en las operaciones de detección de texto cabe citar: i) el Proyecto Artemis de Microsoft[28]; ii) Amazon Rekognition[29]; iii) la tecnología Spirit AI de Twitch[30]; iv) el clasificador basado en el aprendizaje automático de clasificación de Meta (que combina tecnología de análisis interno del lenguaje con metadatos); v) el filtrado de chats de Roblox[31]; vi) herramienta de Yubo para la detección de la captación de menores; vii) herramienta de detección de textos de Safer Predict[32]; y viii) Text Moderation de Hive[33].

Yubo ha informado de que la tasa de precisión de la detección de captación de menores basada en texto en sus servicios alcanzó una media del 87 %[34], lo que significa que, de cien casos de sospecha de captación de menores señalizados automáticamente a moderadores humanos, se confirmó que ochenta y siete correspondían a captación de menores. Los estudios muestran que los métodos de aprendizaje automático para detectar la captación de menores en línea pueden alcanzar una precisión del 92 % y destacan en la percepción de patrones complejos y no lineales esenciales para analizar interacciones en línea matizadas[35].

La herramienta Safer Predict Text Detection utiliza un modelo de clasificación de textos de aprendizaje automático para detectar la explotación sexual de menores. Analiza textos y asigna una puntuación de riesgo basada en la probabilidad de que el contenido se asocie a comportamientos nocivos, como mensajes relacionados con el intercambio de MASM, en

---

28 El Proyecto Artemis de Microsoft se desarrolló en colaboración con The Meet Group, Roblox, Kik y Thorn.

29 Amazon, Amazon 'Rekognition'. Véase también Amazon, *What is Amazon Rekognition?*, consultado el 26 de mayo de 2025.

30 Para más información, véase: Twitch, *Our Ongoing Work to Combat Online Grooming*, 22 de noviembre de 2022, consultado el 26 de mayo de 2025.

31 Roblox filtra publicaciones y chats para jugadores de 12 años o menos a fin de detectar contenidos inadecuados e impedir la publicación de información personal, como por ejemplo direcciones de domicilios. Este sistema de filtrado abarca todos los ámbitos de comunicación en Roblox, públicos y privados. Roblox, *Safety Features: Chat, Privacy & Filtering*, consultado el 26 de mayo de 2025.

32 Véase: Safer, *Enhancing Platform Safety: insights from Safer Predict's Text Detection Beta Period*, 29 de julio de 2024, y *Announcing Safer Predict: AI-Driven CSAM & CSE Detection*, 19 de julio de 2024, consultado el 26 de mayo de 2025.

33 Hive Moderation, *Automated Models with a human-level understanding of textual content* y *Text Moderation - Overview*, consultado el 26 de mayo de 2025. El modelo de clasificación de textos se entrena con un amplio corpus propio de datos etiquetados en múltiples ámbitos (incluidos, entre otros, las redes sociales, los chats y las aplicaciones de retransmisión en directo), y es capaz de interpretar frases completas con sutilezas lingüísticas. Los algoritmos de asociaciones buscarán frases para un conjunto de comportamientos predefinidos que suelen asociarse a contenidos nocivos, incluido el ASM.

34 Yubo, *SAM EU Reporting obligations*, 31 de enero de 2025, consultado el 26 de mayo de 2025. Según Yubo, la exactitud se calcula como el número de casos señalizados automáticamente como captación de menores que se confirmaron como tales tras una revisión humana.

35 Leiva-Bianchi M. *et al*. (eds.), *Effectiveness of machine learning methods in detecting grooming: a systematic meta-analytic review* [«Eficacia de los métodos de aprendizaje automático en la detección de la captación de menores: una revisión metanalítica sistemática», en inglés], *Scientific Reports 15*, n.º 9008, 2025. El estudio presenta una revisión sistemática y un metanálisis del uso de métodos de aprendizaje automático para detectar la captación de menores en línea. Los resultados ponen de relieve la eficacia de determinados algoritmos y contribuyen a la detección de los depredadores en línea. El estudio define «exactitud» como la indicación de la corrección general del modelo en sus predicciones, y la precisión como el número de casos positivos detectados con precisión.

particular los contenidos autogenerados, y mensajes relacionados con el abuso de menores fuera de línea y actividades de sextorsión.

Se están desarrollando otras herramientas de IA para luchar contra la captación de menores en línea. Por ejemplo, el proyecto CESAGRAM de Missing Children Europe, que está dedicado a comprender e impedir el funcionamiento de los mecanismos que subyacen a la captación de menores, tiene previsto producir una herramienta de IA que contribuya a prevenir la captación de menores, sirviéndose de análisis lingüísticos para detectar actividades de captación de menores basados en técnicas de procesamiento del lenguaje natural[36].

2.3.4. Uso de la IA generativa con fines de ASM

El panorama de amenazas relacionadas con el uso indebido de la IA generativa con fines de ASM ha evolucionado rápidamente en los últimos años. Las herramientas de IA generativa ampliamente disponibles pueden utilizarse como arma para hacer daño a los niños, y el uso de la tecnología en la explotación sexual de menores ha aumentado. Esta tecnología puede utilizarse para crear o modificar imágenes, facilitar directrices sobre cómo captar menores o abusar de ellos, o incluso simular la experiencia de un chat explícito con un menor. En 2024, el NCMEC informó de un aumento del 1 325 % en las denuncias que implicaban IA generativa: de 4 700 informes en 2023 a 67 000 en 2024[37]. Además, en un estudio aislado de la IWF de un foro de MASM en la web oscura se hallaron más de 20 000 imágenes generadas por IA publicadas en un período de un mes, en las que más de 3 000 mostraban actividades delictivas de ASM[38].

Los delincuentes utilizan la IA generativa para explotar a los menores de diversas maneras, como las que se enumeran a continuación[39].

- Texto a texto: utilizar instrucciones de texto para generar guías, tutoriales o sugerencias sobre cómo captar a menores y abusar sexualmente de ellos.
- Texto a imagen: introducir instrucciones de texto para generar MASM nuevo o modificar archivos cargados previamente para hacerlos sexualmente explícitos.
- Imagen a imagen (alteración del MASM conocido para crear MASM nuevo): cargar MASM conocido para generar MASM nuevo basado en imágenes existentes, en particular alterando o añadiendo nuevos elementos de abuso (por ejemplo, ataduras u otras formas de abuso) a las imágenes existentes.
- Imagen a imagen (alteración de una imagen inocua para crear una imagen de explotación): cargar imágenes inocuas de un menor para generar imágenes sexualmente explícitas o de

[36] Para más información, véase Missing Children Europe, CESAGRAM, consultado el 26 de mayo de 2025.
[37] NCMEC, *2024 CyberTipline Report*, 2024, consultado el 26 de mayo de 2025.
[38] Internet Watch Foundation, *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, consultado el 26 de mayo de 2025.
[39] NCMEC, *Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism*, «Ending the Scourge: the need for the STOP CSAM Act» [«Acabar con la lacra: la necesidad de la Ley anti- MASM», documento en inglés], 11 de marzo de 2025, pp. 2-4.

explotación del menor (por ejemplo, aplicaciones de desnudo). La IA generativa también se utiliza de este modo para perpetrar sextorsiones económicas contra los menores.

El NCMEC ha señalado la falta de protocolos de seguridad regulados, la velocidad a la que han proliferado las herramientas de IA generativa a través de aplicaciones, plataformas y el acceso de código abierto, y la relativa facilidad con que puede utilizarse esta tecnología. Además, la proliferación del ASM generado por IA plantea retos nuevos y relevantes para las fuerzas y cuerpos de seguridad, también en lo que respecta a la identificación de las víctimas, debido a la dificultad de determinar si las imágenes son reales o sintéticas, lo que, a su vez, puede desviar esfuerzos de los casos que afectan a niños reales que necesitan protección urgente[40].

3. CONCLUSIONES

Medidas de aplicación adoptadas por los proveedores

Los informes de los proveedores revelaron que estos han venido detectando y denunciando el ASM en línea en virtud del Reglamento utilizando diversas tecnologías y procesos de detección. Todos los proveedores informaron del envío de estas denuncias al NCMEC. Para el año 2024, los proveedores incumplieron su obligación de presentar el informe sobre el tratamiento de datos personales utilizando el formulario normalizado establecido en el acto de ejecución de la Comisión adoptado el 25 de noviembre de 2024. Como consecuencia de ello, los informes presentados siguen acusando deficiencias que afectan a la comparabilidad general de los datos.

Medidas de aplicación adoptadas por los Estados miembros

Los informes presentados por los Estados miembros siguen planteando problemas similares a los señalados en el primer informe sobre la aplicación del Reglamento. Los datos presentados por los Estados miembros parecen incompletos y fragmentados. Por lo tanto, no es posible ofrecer una visión global y fiable del número de denuncias de ASM en línea detectados, del número de menores identificados y del número de infractores condenados. Las disparidades entre los datos del NCMEC y los datos de los Estados miembros confirman que la recogida de datos y la presentación de informes por parte de los Estados miembros siguen acusando deficiencias significativas.

Consideraciones generales

En términos generales, el presente informe muestra notables disparidades en la presentación de datos relativos a la lucha contra el ASM en línea en virtud del Reglamento, tanto por parte de los proveedores como de los Estados miembros. Es necesaria una mayor normalización de los datos disponibles y su notificación.

---

[40] NCMEC, *Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism*, «Ending the Scourge: the need for the STOP CSAM Act» [«Acabar con la lacra: la necesidad de la Ley anti- MASM», documento en inglés], 11 de marzo de 2025, p. 4.

Los datos disponibles revelan que, si bien los materiales señalizados automáticamente como posibles MASM se confirman como tales de forma abrumadora tras una revisión humana, una pequeña fracción puede no ser MASM tras esta revisión. Si bien la tasa de falsos positivos es tan baja como 1 entre 50 000 millones en el caso de algunas herramientas, esta fracción también depende de la decisión del proveedor de adaptar la configuración de la precisión de la herramienta para minimizar los falsos negativos, con el consiguiente aumento de falsos positivos para su filtrado posterior mediante revisión humana.

Los datos también muestran grandes variaciones en el número de solicitudes de revisión y las tasas de éxito de estas, de lo cual no es posible extraer conclusiones, dada la falta de información compartida por los proveedores sobre, en particular, el alcance de las solicitudes de revisión y los motivos para el restablecimiento.

Por lo que se refiere a los requisitos del artículo 9, apartado 2, sobre las condiciones para el tratamiento de datos, la información facilitada indica que las tecnologías utilizadas corresponden a aplicaciones tecnológicas diseñadas con el único propósito de detectar y retirar el MASM en línea y denunciarlo ante las autoridades policiales y las organizaciones que actúan en interés público contra el ASM. Los proveedores no facilitaron información sobre si las tecnologías se habían aplicado de acuerdo con el estado actual de la técnica y de la manera menos invasiva para la intimidad, ni sobre si se habían llevado a cabo una evaluación de impacto previa relativa a la protección de datos, conforme a lo indicado en el artículo 35 del Reglamento (UE) 2016/679, y un procedimiento de consulta previa, conforme al artículo 36 de dicho Reglamento.

Por lo que respecta a la proporcionalidad del Reglamento (UE) 2021/1232, la cuestión es si el Reglamento logra el equilibrio pretendido entre, por un lado, alcanzar la consecución del objetivo de interés general de combatir de manera efectiva los delitos de extrema gravedad que aquí nos ocupan y la necesidad de proteger los derechos fundamentales de los menores (por ejemplo, dignidad, integridad, prohibición de un trato inhumano o degradante, vida privada, derechos del niño, etcétera) y, por otro, la salvaguardia de los derechos fundamentales de los usuarios de los servicios contemplados (por ejemplo, intimidad, protección de los datos personales, libertad de expresión, tutela judicial efectiva, etcétera). Los datos disponibles son insuficientes para dar una respuesta definitiva a esta pregunta. No es posible ni conveniente aplicar una norma numérica a la hora de evaluar dicha proporcionalidad en función del número de menores rescatados, habida cuenta del significativo impacto negativo que causan los abusos sexuales en la vida y los derechos de un menor. No obstante, habida cuenta de lo anterior, no hay indicios de que la excepción no sea proporcionada.

Si bien las deficiencias de los datos no permiten tener una imagen completa, los datos disponibles muestran que se identificaron miles de niños en el período de notificación y que se retiraron de la circulación millones de imágenes y vídeos, lo que redujo la victimización secundaria. Por lo tanto, la denuncia voluntaria en consonancia con el presente Reglamento parece contribuir considerablemente a la protección de un gran número de menores, también frente a los abusos continuados.

Al mismo tiempo, en la propuesta de Reglamento de la Comisión por el que se establecen normas para prevenir y combatir el abuso sexual de los menores se han abordado importantes deficiencias detectadas en la aplicación del presente Reglamento, como una mayor normalización de los datos disponibles y, por lo tanto, de la presentación de informes, con el fin de obtener una visión más clara de las actividades pertinentes en la lucha contra este delito, así como el uso de indicadores específicos para detectar MASM ilegal y la verificación del material por parte de un centro independiente[41]. Su adopción por los colegisladores sigue siendo una prioridad. Es esencial garantizar que no surjan lagunas jurídicas entre el marco jurídico existente y el futuro marco jurídico mejorado, y que, mientras tanto, el actual siga aplicándose de la manera más eficaz posible.

[41] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores [COM(2022) 209 final].