



Bruselas, 19.12.2023
COM(2023) 797 final

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

LISTA DE TÉRMINOS Y SIGLAS	2
1. INTRODUCCIÓN	4
2. MEDIDAS DE APLICACIÓN.....	5
2.1. Tratamiento de datos personales por parte de los proveedores [artículo 3, letra g), inciso vii)]	5
2.1.1. Tipo y volumen de datos tratados	5
2.1.2. Motivos para el tratamiento de conformidad con el Reglamento (UE) 2016/679	6
2.1.3. Motivo para las transferencias de datos personales fuera de la Unión de conformidad con el capítulo V del RGPD, en su caso.....	7
2.1.4. Número de casos detectados de abusos sexuales de menores en línea, diferenciando entre MASM y embaucamiento de menores.....	8
2.1.5. Recursos de usuarios y resultado	9
2.1.6. Número y tasas de errores (falsos positivos) de las diferentes tecnologías utilizadas	11
2.1.7. Medidas aplicadas para limitar la tasa de error y la tasa de error alcanzada.....	14
2.1.8. Política de conservación de los datos y salvaguardias de protección de datos aplicadas conforme al RGPD.....	15
2.1.9. Nombre de las organizaciones que actúan en interés público contra los abusos sexuales de menores con las que se hayan compartido datos en virtud del Reglamento	16
2.2. Estadísticas de los Estados miembros (artículo 8)	17
2.2.1. Número total de denuncias de abusos sexuales de menores en línea detectados	18
2.2.2. Número de menores identificados.....	26
2.2.3. Número de infractores condenados.....	29
2.3. Avances tecnológicos	32
2.3.1. Detección de MASM conocido.....	32
2.3.2. Detección de MASM nuevo.....	33
2.3.3. Detección de la captación de menores	34
2.3.4. Nuevos retos planteados por los robots conversacionales y los generadores de arte o imágenes basados en la inteligencia artificial	35
3. CONCLUSIONES.....	37

LISTA DE TÉRMINOS Y SIGLAS

Término/Sigla	Definición
IA	Inteligencia artificial
API	Interfaz de programación de aplicaciones (por sus siglas en inglés)
ChatGPT	ChatGPT (Chat Generative Pre-trained Transformer, Chat Transformador Generativo Preentrenado) es una forma de IA generativa. Se trata de un robot conversacional basado en un gran modelo de lenguaje, desarrollado por OpenAI, que permite a los usuarios perfilar y dirigir una conversación para obtener la longitud, el formato, el estilo, el nivel de detalle y el lenguaje deseados.
Clasificador	Una forma de inteligencia artificial consistente en un algoritmo que organiza datos por clases o categorías etiquetadas.
Clasificador Content Safety API	El clasificador Content Safety API de Google se sirve del acceso mediante programación y de la inteligencia artificial para ayudar a clasificar y ordenar por prioridad miles de millones de imágenes para su revisión.
ASM	Abuso sexual de menores
CSAI Match	CSAI Match es una tecnología desarrollada por los ingenieros de YouTube para detectar copias cargadas de nuevo de vídeos en los que ya se hubieran detectado anteriormente abusos sexuales de menores.
MASM	Material de abuso sexual de menores, p. ej., imágenes y vídeos que representen ASM
Directiva ASM	Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo (DO L 335 de 17.12.2011, p. 1)
EASM	Explotación y abusos sexuales de menores
ASM en línea	Término común utilizado para referirse a los tres tipos de abuso sexual de menores, definidos en la Directiva ASM, a saber: pornografía infantil, espectáculo pornográfico y embaucamiento de menores («captación de menores»), tal como se definen en el Reglamento provisional (artículo 2, punto 4).
UE	Unión Europea
RGPD	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)

Captación de menores	Conducta por la que el infractor se gana la confianza de un menor y entabla una relación con este para acercarse a él con fines de explotación o abuso sexual. Formalmente conocido como «embaucamiento de menores», tal como se define en el artículo 6 de la Directiva ASM.
Hash	Código digital único creado por un algoritmo matemático («hashing»), que se convierte en la firma de un archivo o en su valor resumen.
Reglamento provisional	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).
LLM	Un gran modelo de lenguaje (LLM, por sus siglas en inglés) es un tipo de modelo de inteligencia artificial entrenado mediante algoritmos de aprendizaje profundo para reconocer, generar, traducir o resumir vastas cantidades de lenguaje humano escrito y datos textuales.
MD5	Algoritmo criptográfico de cálculo de códigos de autenticación de mensajes concebido para usarse en internet.
SSN++ de Meta	Modelo de IA, desarrollado por Meta, capaz de detectar duplicados casi exactos.
NCMEC	Centro Nacional para Niños Desaparecidos y Explotados (organización privada estadounidense sin ánimo de lucro), ante el que los proveedores de servicios en línea deben denunciar, con arreglo al Derecho de los EE. UU., los casos de posible abuso sexual de menores que detecten en sus redes.
PDQ y TMK+PDQF	Herramientas usadas por Facebook para detectar contenidos nocivos. PDQ es una tecnología de coincidencia de fotografías; TMK+PDQF es una tecnología de coincidencia de vídeos.
PhotoDNA	La herramienta basada en tecnología de funciones de resumen (<i>hashing</i>) más ampliamente utilizada, disponible de forma gratuita, sobre la base de un acuerdo de concesión de licencias ajustado para evitar usos indebidos o con cualquier otro fin que no sea la detección de ASM.

1. INTRODUCCIÓN

El artículo 9 del Reglamento provisional (en lo sucesivo también, «el Reglamento») obliga a la Comisión a elaborar un informe sobre su aplicación, a partir de los informes presentados por los proveedores de servicios de comunicaciones interpersonales (en lo sucesivo, «proveedores») sobre el tratamiento de datos personales y de las estadísticas facilitadas por los Estados miembros. De acuerdo con la citada disposición, en el informe de aplicación, la Comisión deberá tomar en consideración, en particular:

- a) las condiciones aplicables para el tratamiento de datos personales pertinentes y de otro tipo en virtud del 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 informe de aplicación previsto en el Reglamento provisional se basa en los datos obtenidos a través de los informes presentados por los proveedores y los Estados miembros con arreglo a su artículo 3, apartado 1, letra g), inciso vii), y su artículo 8, respectivamente. Dichos informes han revelado 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. Dado que el Reglamento no facilita un modelo para los informes, los proveedores compartieron distintos tipos de información que no eran necesariamente comparables; así pues, los servicios de la Comisión llevaron a cabo un seguimiento para garantizar la correcta interpretación de los datos. La mayoría de los Estados miembros no pudieron proporcionar datos a tiempo y algunos de ellos no han logrado facilitar ningún dato hasta la publicación del presente informe. Esto ha afectado significativamente a los plazos, la exhaustividad y la utilidad del informe. Pese a los esfuerzos por garantizar la coherencia de los datos y su comparabilidad, siguen existiendo notables diferencias que se reflejan en los cuadros que figuran más adelante, los cuales tampoco contienen datos relativos a todos los proveedores o Estados miembros acerca de todos los aspectos.

El presente informe de aplicación tiene por objeto ofrecer una visión general basada en hechos de la situación actual por lo que respecta a la aplicación del Reglamento provisional, 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, letra g), inciso vii)]

En el artículo 3, letra g), inciso vii), del Reglamento provisional 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 X (anteriormente Twitter)¹ presentaron informes referentes a 2021 y 2022.

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 abusos sexuales de menores en línea, todos los proveedores anteriormente citados mencionaron imágenes y vídeos. Se sirvieron principalmente de las tecnologías de coincidencia de *hashes* PhotoDNA y MD5 para detectar coincidencias con el material de abuso sexual de menores (en lo sucesivo, «MASM») anteriormente detectado. La herramienta CSAI Match de Google se utilizó para crear huellas digitales de vídeos disponibles en plataformas y compararlas con los archivos almacenados en el repositorio de huellas de Google/YouTube (LinkedIn). El uso de tecnología automatizada (aprendizaje automático mediante inteligencia artificial) y de la revisión humana también fue notificado (por ejemplo, por parte de Google). Google y LinkedIn confirmaron asimismo la detección de MASM que no coincidía con el MASM anteriormente detectado. Ninguno de los cinco proveedores que presentaron información facilitó datos sobre la detección de embaucamiento de menores a través del reconocimiento de texto dentro del ámbito de aplicación de la excepción prevista en el Reglamento.

En cuanto a los datos de tráfico recogidos y los correspondientes volúmenes de los distintos tipos de datos de contenido y de tráfico tratados, los informes de los proveedores variaban notablemente.

Entre los datos de tráfico recogidos por los proveedores e incluidos en las denuncias presentadas a través de CyberTipline ante el Centro Nacional para Niños Desaparecidos y Explotados (en lo sucesivo, NCMEC), figuran (la totalidad o una selección de) los siguientes datos:

- a) datos relacionados con el usuario / el denunciado/ la cuenta (Google, LinkedIn, Microsoft y X);
- b) metadatos relacionados con los datos de contenido/transacciones (Google, LinkedIn y Microsoft);

¹ Twitter presentó su contribución antes de su cambio de nombre; en el resto del presente informe se denominará «X».

- c) datos relacionados con una posible víctima (Google);
- d) datos de operaciones de abuso (Google).

En términos de volúmenes de datos tratados en virtud del Reglamento provisional, LinkedIn informó del tratamiento de ocho millones de imágenes y vídeos procedentes de la UE entre el 14 de julio y el 31 de diciembre de 2021, y 21 millones de imágenes y 63 000 vídeos procedentes de la UE en 2022. Microsoft informó del tratamiento, a efectos del Reglamento, de 8 900 millones de imágenes y vídeos de todo el mundo entre julio y diciembre de 2021, y 12 300 millones de elementos de contenido de todo el mundo en 2022; no había disponibles cifras de la UE, por lo que no es posible extraer ninguna conclusión a efectos del presente informe. Los demás proveedores no facilitaron información sobre los volúmenes de datos tratados. Por tanto, de los cinco proveedores que presentaron informes, solo uno facilitó datos con el nivel de detalle requerido.

Para ilustrar el contexto global, el NCMEC informó de haber recibido un total de 87,2 millones de imágenes y vídeos de todo el mundo y 5,1 millones de imágenes y vídeos que incumbían a la UE en 2022, así como 84,8 millones de imágenes y vídeos de todo el mundo y 1,8 millones de imágenes y vídeos que incumbían a la UE en 2021. Estas cifras se refieren únicamente al material identificado por un proveedor como posible MASM y, por consiguiente, no pueden considerarse indicativas de los volúmenes globales de datos tratados en virtud del Reglamento provisional.

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

Los proveedores informaron de que invocaron los siguientes motivos específicos de conformidad con el Reglamento (UE) 2016/679 (en lo sucesivo, RGPD):

- el artículo 6, apartado 1, letra d), del RGPD, esto es, el tratamiento necesario para proteger los intereses vitales de los menores y de las víctimas de abusos sexuales de menores en línea (Google, Meta y X²);
- el artículo 6, apartado 1, letra e), del RGPD, esto es, el tratamiento necesario para el cumplimiento de misiones realizadas en interés público (LinkedIn, Microsoft, Meta y X³);
- el artículo 6, apartado 1, letra f), del RGPD, esto es, el tratamiento necesario para la satisfacción de los intereses legítimos de:
 - i. el proveedor en detectar, prevenir o hacer frente de otro modo al abuso sexual de menores en línea en sus servicios y proteger a otros usuarios, clientes, socios y el público de esta forma de contenidos ilícitos (Google y Meta);
 - ii. las víctimas de abuso sexual de menores y la organización ante la que el proveedor denuncie el abuso sexual de menores (p. ej., el NCMEC) en que se

² Meta y X no especificaron el artículo concreto.

³ Meta y X no especificaron el artículo concreto.

detecte, prevenga y retire el material de abuso sexual de menores de sus servicios (Google).

2.1.3. Motivo para las transferencias de datos personales fuera de la Unión de conformidad con el capítulo V del RGPD, en su caso

Todos los proveedores informaron de haberse acogido a cláusulas contractuales tipo aprobadas por la Comisión con arreglo al artículo 46, apartado 2, letra c), del RGPD. Por lo que respecta a las transferencias de datos personales al NCMEC, LinkedIn también informó de haberse acogido a una excepción, en la medida en que esta era aplicable, permitida en virtud del artículo 49, apartado 1, del RGPD.

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

Cuadro n.º 1: Número de casos de abusos sexuales de menores en línea detectados en 2021

Proveedor	Número de casos de MASM detectados en 2021	Observaciones
Google	33 cuentas de Google Chat	Se refiere al número de cuentas de Google Chat de usuarios de la UE en las que se detectaron abusos sexuales de menores mediante tecnologías automatizadas en el período comprendido entre el 2 de agosto y el 31 de diciembre de 2021. No se facilitaron datos sobre el número de elementos de contenido detectados.
LinkedIn	31 elementos de contenido	Mediante la revisión manual, se confirmó la existencia de 31 elementos de contenido que constituían MASM y que se denunciaron ante el NCMEC; 6 eran MASM conocido y los 25 restantes, MASM desconocido.
Meta	340 000 cuentas	Número de cuentas en las que se detectó el envío de al menos un elemento multimedia que constituía MASM, en hilos de mensajes que incluían a un usuario de la UE, entre el 8 de noviembre y el 31 de diciembre de 2021.
Microsoft	6 600 elementos de contenido	6 600 elementos de contenido (imágenes o vídeos individuales) confirmados como MASM procedente de la UE de entre los más de 20 000 elementos de contenido detectados a escala mundial entre julio y diciembre de 2021.
X (anteriormente Twitter)	532 898 cuentas	Cuentas (no queda claro si únicamente de la UE o de todo el mundo) suspendidas entre el 2 de agosto y el 31 de diciembre de 2021 por violar la política de X contra la explotación sexual de menores.

En el caso de X, no queda claro si los datos facilitados se refieren exclusivamente a servicios que entran dentro del ámbito de aplicación del Reglamento provisional (servicios de comunicaciones interpersonales independientes de la numeración) o si esa cifra también incluye otros servicios (como los servicios de la sociedad de la información). Esto afecta a todos los datos relacionados con X reflejados en el presente informe.

Cuadro n.º 2: Número de casos de abusos sexuales de menores en línea detectados en 2022

Proveedor	Número de casos de MASM detectados en 2022	Observaciones
Google	2 045 elementos de contenido	Elementos de contenido correspondientes a usuarios de la UE detectados en 752 cuentas de Google a través de tecnologías automatizadas y denunciados ante el NCMEC.

LinkedIn	2 elementos de contenido	LinkedIn detectó 2 imágenes y 0 vídeos confirmados como MASM.
Meta	6,6 millones de elementos de contenido	Elementos multimedia que constituían MASM y que fueron objeto de medidas, detectados usando la tecnología de coincidencia de publicaciones mediáticas de Meta, en hilos de mensajes que incluían a un usuario de la UE.
Microsoft	12 800 elementos de contenido	12 800 elementos de contenido (imágenes o vídeos individuales) confirmados como MASM procedente de la UE de entre los más de 50 000 elementos de contenido detectados a escala mundial en 2022.
X (anteriormente Twitter)	2 348 712 cuentas	Cuentas (no queda claro si únicamente de la UE o de todo el mundo) suspendidas por violar la política de X contra la explotación sexual de menores.

2.1.5. Recursos de usuarios y resultado

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

Los proveedores informaron de la implantación de dichos procedimientos y mecanismos de recurso interno para los usuarios cuyas cuentas se hayan restringido por haber compartido MASM o cuyo contenido se haya retirado por considerarse MASM, de forma que puedan recurrir dicha restricción o retirada y hacer que su caso se revise por si se hubieran cometido errores.

Estos notificaron los casos en los que un usuario había presentado una reclamación ante el mecanismo de recurso interno o ante una autoridad judicial en relación con algún asunto contemplado en el ámbito de aplicación del Reglamento y acaecido dentro de la UE, y el resultado de dichas reclamaciones. Ningún proveedor salvo Microsoft (que notificó cero reclamaciones por ambas vías en 2021 y 2022) proporcionó estadísticas por separado sobre los recursos internos y los recursos judiciales; como consecuencia de ello, los cuadros que figuran a continuación abarcan los procedimientos de recurso tanto interno como judicial.

Cuadro n.º 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 2021

Proveedor	Número de casos de reclamaciones de usuarios	Número de cuentas restablecidas	Número de elementos de contenido restablecidos	Observaciones
Google	8	0	n. d.	Cuentas de Google Chat desactivadas por abuso sexual de menores en línea sobre las

				que el usuario presentó un recurso: 8. No se restableció ninguna.
LinkedIn	0	n. d.	n. d.	
Meta	4 900	n. d.	207	4 900 usuarios presentaron un recurso. Tras el procedimiento de recurso, se restableció el contenido de 207 usuarios y se revirtieron las medidas tomadas respecto a las cuentas.
Microsoft	0	n. d.	n. d.	
X (anteriormente Twitter)	90 000 aprox.	3 000 aprox.	n. d.	90 000 reclamaciones aprox. X restableció unas 3 000 cuentas.

Cuadro n.º 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 2022

Proveedor	Número de casos de reclamaciones de usuarios	Número de cuentas restablecidas	Número de elementos de contenido restablecidos	Observaciones
Google	378	0	n. d.	Cuentas de Google desactivadas por abuso sexual de menores en línea sobre las que el usuario presentó un recurso: 378. No se restableció ninguna.
LinkedIn	0	n. d.	n. d.	
Meta	29 000	n. d.	3 700	Los usuarios recurrieron las medidas tomadas en relación con unos 29 000 elementos de sus medios compartidos. Tras el procedimiento de recurso, se restablecieron unos 3 700 elementos de contenido, y se

				revirtieron las medidas tomadas respecto a las cuentas.
Microsoft	0	n. d.	n. d.	
X (anteriormente Twitter)	430 000 aprox.	4 000 aprox.	n. d.	430 000 recursos aprox. X restableció unas 4 000 cuentas.

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 provisional, 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 abusos sexuales de menores en línea.

A este respecto, los proveedores informaron de que no aplican aisladamente cada tecnología para detectar el ASM en línea. En su lugar, aplican un enfoque por niveles para detectar ASM en línea combinando distintas tecnologías de detección a fin de aumentar la precisión. Con objeto de reducir el número de errores o falsos positivos, todos los proveedores las complementan con la revisión humana. Los proveedores no facilitaron el número y las tasas de errores (falsos positivos) de cada una de las tecnologías utilizadas por separado, sino que comunicaron datos agregados sobre el conjunto de tecnologías utilizadas.

La mayoría de los proveedores miden el número y las tasas de errores en función de la revocación de decisiones de ejecución, es decir, la tasa general de restablecimiento/revocación tras presentar un recurso (p. ej., la tasa de cuentas o contenidos desactivados y posteriormente restablecidos por el proveedor tras un recurso del usuario). El enfoque adoptado por los proveedores no refleja necesariamente la definición de «falsos positivos» en las estadísticas.

Las tasas de restablecimiento/revocación tras presentar un recurso son las siguientes:

Cuadro n.º 5: Tasas de restablecimiento/revocación tras presentar un recurso

Proveedor	2021*		2022		Observaciones
	% de cuentas restablecidas frente al número de recursos	% de cuentas restablecidas frente al número de cuentas suspendidas	% de cuentas restablecidas frente al número de recursos	% de cuentas restablecidas frente al número de cuentas suspendidas	
Google	0 % (0 frente a 8)	0 % (0 frente a 33)	0 % (0 frente a 378)	0 % (véanse las observaciones)	No se facilitó el número de cuentas suspendidas en 2022. En su lugar, se facilitó el número de elementos de contenido detectados y denunciados ante el NCMEC, 2 045. No se restableció ninguna cuenta tras la presentación de un recurso.
LinkedIn	0 %	0 %	0 %	0 %	No hubo recursos. Entre el 13 de julio y el 31 de diciembre de 2021, LinkedIn también informó de que, de los 75 expedientes revisados por constituir posible MASM procedente de la UE, 31 fueron confirmados como tales mediante revisión humana. LinkedIn no facilitó tales datos respecto a 2022.
Meta	4,22 % (207 frente a 4 900)	0,06 % (207 frente a 340 000)	Véanse las observaciones	Véanse las observaciones	No se facilitó información para determinar con precisión el alcance, el contenido de los recursos ni los motivos del restablecimiento. Respecto a 2022, los datos facilitados se referían a elementos de contenido, no a cuentas: - número de elementos de contenido suspendidos («objeto de medidas»): 6,6 millones, - número de elementos de contenido objeto de recurso: 29 000, - número de elementos de contenido restablecidos:

					<p>3 700.</p> <p>Por consiguiente:</p> <ul style="list-style-type: none"> - % de elementos de contenido restablecidos frente al número de recursos: 12,8 % (3 700 frente a 29 000), - % de elementos de contenido restablecidos frente al número de elementos de contenido suspendidos: 0,06 % (3 700 frente a 6,6 millones).
Microsoft	0 %	-	-	-	Datos insuficientes para permitir el cálculo de la tasa de restablecimiento/revocación tras presentar un recurso. Por lo que respecta al total de 17 revocaciones en 2022 de decisiones iniciales de moderación de contenidos, no se facilitaron cifras sobre el total de recursos.
X (anteriormente Twitter)	1,43 % (100 frente a 7 000)	0,06 % (100 frente a 166 000)	2,17 % (500 frente a 23 000)	0,10 % (500 frente a 501 000)	<p>En el segundo semestre de 2021, unos 166 000 usuarios fueron suspendidos por ASM por medio de mecanismos automatizados. De estos usuarios, unos 7 000 presentaron recursos que dieron lugar a unas 100 revocaciones.</p> <p>En 2022, 501 000 usuarios fueron suspendidos por ASM por medio de mecanismos automatizados. De estos usuarios, unos 23 000 presentaron recursos que dieron lugar a unas 500 revocaciones.</p>

* Los períodos de notificación en 2021 varían según el proveedor.

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 provisional, 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 la supervisión y, en caso necesario, la intervención humana.

Todos los proveedores informaron de haber utilizado un enfoque por niveles para detectar y combatir la difusión de ASM en línea. Este abarca el uso de tecnologías de coincidencia de *hashes* (como PhotoDNA) para detectar MASM, en combinación con procesos de revisión humana para confirmar si un archivo multimedia (imagen o vídeo) contiene MASM, así como la supervisión humana del tratamiento de dicho material.

Los proveedores notificaron la aplicación de diferentes medidas y salvaguardias para limitar y reducir la tasa de error en su proceso de detección, denuncia y retirada de ASM en línea. Entre dichas medidas se incluyen las siguientes (lista no exhaustiva)⁴:

- 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 abuso sexual de menores en línea) y a modo de recordatorio (de que no están pasando por alto abusos sexuales de menores en línea en sus plataformas) (Google y X);
- ii. la revisión y supervisión humanas: muestras de medios detectados como MASM por tecnologías de coincidencia de *hashes* son auditadas por revisores humanos / analistas formados (Google, LinkedIn, Meta y Microsoft);
- iii. la señalización y la revisión de agrupaciones de un volumen elevado (Meta);
- iv. la implantación de nuevos procesos de revisión manual, como controles de calidad de *hashes* en curso (LinkedIn y Microsoft);
- v. los revisores humanos que reciben formaciones sólidas especializadas, bajo la dirección de asesores, sobre cómo reconocer el contenido que constituye MASM a fin de garantizar la exactitud de la revisión humana (Google);
- vi. las evaluaciones periódicas de control de la calidad de los revisores humanos y de los veredictos que se aplican (Google y X);
- vii. otros procesos de control de la calidad para reducir los errores y rectificarlos de inmediato, como la verificación de *hashes* independiente (Google y LinkedIn) o la revisión humana de cada caso de MASM nunca antes detectado, con anterioridad a su denuncia (Google);
- viii. la elaboración y la revisión periódica de políticas y estrategias de ejecución a cargo de expertos formados en materia de ASM en línea (Google);

⁴ Los proveedores indicados entre paréntesis son los que notificaron específicamente las medidas en cuestión. Si algunos proveedores no figuran en la lista, no significa que no hayan aplicado esa medida, sino únicamente que no la mencionaron en su informe.

- ix. la implicación en lo que respecta a la calidad y los falsos positivos, si los hubiera, de las denuncias presentadas ante el NCMEC a través de CyberTipline (Google, LinkedIn, Meta, Microsoft y X).

2.1.8. Política de conservación de los datos y salvaguardias de protección de datos aplicadas conforme al RGPD

Las letras h) e i) del artículo 3, apartado 1, del Reglamento provisional 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.

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. Estos señalan que, en cada caso, el período de conservación está limitado en el tiempo, conforme a lo que se estima adecuado para el tipo de datos y la finalidad del tratamiento, y que los datos se suprimen al final del período de conservación. Los proveedores disponen de información más detallada sobre las prácticas de conservación de datos en sus políticas o declaraciones de confidencialidad y en los acuerdos de servicios o con usuarios.

La mayoría de los proveedores (LinkedIn, Meta y Microsoft) aplican una política de conservación de noventa días de los medios sobre los que se confirma que contienen MASM detectado dentro del ámbito de aplicación del Reglamento. Durante este período, el contenido confirmado como MASM se guarda en un sistema de almacenamiento separado y seguro para este tipo de material, que es gestionado por equipos especializados (p. ej., el Equipo de Garantía del Cumplimiento de la Ley y de Seguridad Nacional de Microsoft). Estos sistemas de almacenamiento suprimen automáticamente al cabo de noventa días el MASM guardado, a menos que el período de almacenamiento se haya ampliado tras la recepción de solicitudes de tratamiento lícito, generalmente relacionadas con la investigación por parte de las fuerzas y los cuerpos de seguridad de una denuncia presentada ante el NCMEC.

Google informó de que el MASM detectado en el ámbito de aplicación del Reglamento no se almacena durante más tiempo del estrictamente necesario para los fines pertinentes previstos en el Reglamento y, en cualquier caso, no durante más de doce meses desde la detección y denuncia del MASM, con la posibilidad de ampliar el plazo sobre la base de una solicitud de conservación legal válida.

X (anteriormente Twitter) informó de que conserva el contenido y la información de los perfiles en tanto la cuenta del usuario está activa, y los datos personales recogidos cuando los usuarios utilizan su servicio durante un máximo de dieciocho meses. Cuando un usuario desactiva su cuenta, X suele conservar los datos durante treinta días adicionales y a continuación se procede a la supresión de la cuenta. Los datos de los usuarios relacionados con denuncias e infracciones de políticas, incluida la información sobre las cuentas de los infractores (p. ej., los identificadores utilizados para crear la cuenta: dirección de correo electrónico o número de teléfono), se conservan indefinidamente para evitar que los infractores de políticas reincidentes creen nuevas

cuentas y para garantizar que los infractores de las políticas de X no puedan limitarse a esperar a que transcurra el período para la supresión y después infringir de nuevo las políticas⁵.

Entre las salvaguardias para la protección de datos personales aplicadas por los proveedores se incluyen las medidas normalizadas del sector (la totalidad o una selección de ellas), como por ejemplo (lista no exhaustiva)⁶:

- i. el uso de técnicas de anonimización o seudonimización de los datos (p. ej., enmascaramiento, *hashing*, privacidad diferencial) (Google, LinkedIn, Meta y Microsoft);
- ii. la facilitación únicamente de los valores resumen a terceros a efectos de la detección de MASM (Google y LinkedIn);
- iii. la aplicación del cifrado normalizado del sector (algoritmos y protocolos) a los datos en tránsito entre infraestructuras de propiedad privada y redes públicas (Meta);
- iv. la aplicación de estrategias de gobernanza de los datos o de programas exhaustivos de confidencialidad (X, anteriormente Twitter, y Google), así como de estrictas restricciones internas del acceso a los datos (Meta) (p. ej., aplicadas al personal, los contratistas o los agentes que necesitan la información para tratarla), uso de listas de control del acceso en todas las herramientas de revisión de MASM y prohibiciones de *hashes* (Meta), y estrictas obligaciones contractuales de confidencialidad impuestas a quienes disponen de acceso;
- v. la revisión de las estrategias de anonimización y gobernanza de los datos, esto es, realización de revisiones de la confidencialidad para detectar, abordar y mitigar posibles riesgos de confidencialidad existentes en el proceso de recogida, tratamiento, almacenamiento e intercambio de datos personales, así como revisión de las prácticas de protección (Microsoft);
- vi. el mantenimiento de planes de respuesta a incidentes de seguridad para la supervisión, detección y gestión de posibles vulnerabilidades e incidentes en materia de seguridad en toda la infraestructura (Google y Meta).

2.1.9. Nombre de las organizaciones que actúan en interés público contra los abusos sexuales de menores con las que se hayan compartido datos en virtud del Reglamento.

En ambos períodos de notificación (de julio/agosto a diciembre de 2021 y de enero a diciembre de 2022), todos los proveedores informaron de haber compartido los datos tratados 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

⁵ Política de privacidad de X, «4. Cuánto tiempo conservamos tus datos», disponible en: <https://twitter.com/es/privacy>.

⁶ Los proveedores indicados entre paréntesis son los que notificaron específicamente las medidas en cuestión. Si algunos proveedores no figuran en la lista, no significa que no hayan aplicado esa medida, sino únicamente que no la mencionaron en su informe.

Reglamento provisional, que habían denunciado al NCMEC los abusos sexuales de menores en línea con arreglo al Reglamento⁷.

2.2. Estadísticas de los Estados miembros (artículo 8)

Con arreglo al artículo 8, apartado 1, del Reglamento provisional, los Estados miembros están obligados a facilitar estadísticas sobre los elementos siguientes:

- a) el número total de denuncias de abusos sexuales de menores en línea detectados que hayan presentado los proveedores y las organizaciones que actúan en interés público contra los abusos sexuales de menores 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 abuso sexual de menores 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.

Si bien la mayoría de los Estados miembros proporcionaron al menos información parcial, en muchos de ellos no se habían establecido los sistemas pertinentes de recopilación y notificación de datos. Como consecuencia de ello, cuando se facilitaron estadísticas, estas se referían a períodos de notificación muy diversos y diferían notablemente en términos de granularidad. Algunos Estados miembros presentaron estadísticas anuales desde la fecha de entrada en vigor del Reglamento. La mayoría de ellos notificaron los datos referidos a años naturales, ya que podían no disponer de los medios técnicos necesarios para diferenciar las estadísticas solicitadas por año desde la fecha de entrada en vigor del Reglamento. Algunos Estados miembros no facilitaron ningún dato.

Cabe señalar asimismo que, en algunos casos, los datos estadísticos se obtienen a partir de las denominadas bases de datos actuales, o sistemas de registro secuencial de datos y gestión de casos, es decir, que no se obtienen de auténticos sistemas estadísticos. En ocasiones, las cifras se facilitan a partir de datos dinámicos, lo que significa que estos no son definitivos, sino que están sujetos a cambios. Los cambios se producen, por ejemplo, dependiendo del momento de la extracción (como en Eslovenia y Dinamarca), a medida que se concluyen más investigaciones y asuntos judiciales.

En varios Estados miembros, las autoridades competentes están creando nuevos departamentos para investigar delitos relacionados con el abuso sexual de menores en línea, así como mecanismos centrales de denuncia de abusos sexuales de menores (Letonia y Chequia). Estas medidas deberían contribuir a disponer de estadísticas más exactas en el futuro.

⁷ La información sobre las organizaciones que actúan en interés público a las que los proveedores denuncian los abusos sexuales de menores 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, de conformidad con las obligaciones de la Comisión previstas en el artículo 8, apartado 2, del Reglamento provisional.

Alemania declaró que no podía facilitar ninguna estadística con arreglo al artículo 8, apartado 1, del Reglamento provisional, ya que consideraba que carecía de base jurídica para la detección voluntaria⁸. Sin embargo, la Oficina Penal Federal (BKA) alemana informa en su sitio web de la recepción en 2022 de 89 844 denuncias procedentes del NCMEC, y el NCMEC informa de la remisión de 138 193 denuncias a las autoridades alemanas⁹. Tres Estados miembros no aportaron ningún dato ni justificación por no haber presentado informes con arreglo a dicha disposición (Malta, Portugal y Rumanía).

2.2.1. Número total de denuncias de abusos sexuales de menores en línea detectados

La mayoría de los Estados miembros facilitaron algunas estadísticas sobre el número total de denuncias de abusos sexuales de menores en línea con arreglo al artículo 8, apartado 1, letra a), del Reglamento provisional. Dado que los Estados miembros facilitaron datos referentes a distintos períodos de notificación, no fue posible calcular el número total de denuncias recibidas de abusos sexuales de menores en línea detectados a escala de la UE en un período determinado, como por ejemplo el período de aplicación del Reglamento.

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 los abusos sexuales de menores. Dado que la mayor parte de los proveedores establecidos en los Estados Unidos presentan las denuncias al NCMEC, la mayoría de los Estados miembros informaron de haber recibido la mayor parte o la totalidad de sus 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 indicaron el número de casos abiertos, que es significativamente menor. La diferencia entre las denuncias recibidas y los casos investigados se atribuyó a diversas razones, como, por ejemplo, que la denuncia contenía MASM, pero no incluía suficiente información para abrir una investigación; que las denuncias se fusionan cuando más de una de ellas concierne a un determinado sospechoso, o que el material, si bien mostraba situaciones de explotación, no fue calificado como delictivo con arreglo al Derecho nacional. Además, la mayoría de los Estados miembros no diferenciaba entre el número absoluto de casos y los casos denunciados varias veces. Cuando las denuncias provenían del NCMEC, este ya había clasificado previamente las denuncias presentadas por los proveedores como «susceptibles de ser objeto de medidas» o «informativas». El NCMEC define las denuncias susceptibles de ser objeto de medidas como aquellas que contienen información suficiente para abrir una investigación. Suelen incluir datos del usuario, imágenes y una posible ubicación. Las denuncias se clasifican como «informativas»

⁸ Informe presentado por Alemania de conformidad con el artículo 8 del Reglamento (UE) 2021/1232, recibido el 18 de octubre de 2022. El NCMEC publica todos los datos sobre las denuncias recibidas y las relacionadas con los Estados miembros de la UE, entre ellos Alemania, en sus Informes por país de la CyberTipline. Véase: NCMEC, [Informes por país de la CyberTipline de 2021](#), consultados en julio de 2023; NCMEC, Informes por país de la CyberTipline de 2022, consultados en julio de 2023.

⁹ https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html.

si contienen información insuficiente o si las imágenes se consideran virales y se han denunciado en numerosas ocasiones. En 2022, el NCMEC clasificó el 49 % de las denuncias como «susceptibles de ser objeto de medidas», mientras que el 51 % se clasificaron como «informativas».

Solo unos pocos Estados miembros indicaron el tipo de proveedores en cuyos servicios se habían detectado los abusos sexuales de menores en línea (p. ej., Bélgica, Chequia, Estonia, Francia y Polonia) y solo un Estado miembro facilitó un desglose pormenorizado (Bélgica).

Eslovenia indicó que no podía proporcionar cifras únicamente sobre los delitos investigados a raíz de denuncias presentadas por proveedores y organizaciones, sino solamente cifras relativas a todas las investigaciones de abusos sexuales de menores en línea, independientemente de la fuente de la información que había dado lugar a la apertura de la investigación.

Cuadro n.º 6: Número total de denuncias de abusos sexuales de menores en línea detectados, notificadas por los Estados miembros

País	Período de notificación	Número total de denuncias de abusos sexuales de menores en línea	Fuente de las denuncias	Observaciones
Austria	2021 a 2022	16 311	NCMEC	
Bélgica	1 de agosto de 2021 al 31 de julio de 2022	26 226	Denuncias procedentes de proveedores (redes sociales) y de la línea directa Child Focus	
Bulgaria	2021 a 2022	9 120	Proveedores y línea directa INHOPE a través de «Safenet» y otros.	De ellas, 9 112 alertas se referían a páginas web que contenían MASM, alojadas por proveedores búlgaros.
Croacia	1 de enero de 2021 al 31 de octubre de 2022	9 044	NCMEC	
Chipre	1 de julio de 2021 al 31 de diciembre de 2022	3 570	NCMEC	
Chequia	1 de enero de 2022 al 31 de julio de 2022	13 279	NCMEC	
Dinamarca	2 de agosto de 2021 al 20 de enero de 2023	10 744	NCMEC	
Estonia	-	-	NCMEC, Child Helpline 116 111	Estonia informó de que las estadísticas de la Policía y la guardia de fronteras, entre ellas las del NCMEC, no son públicas. Respecto a 2021, denunciaron 360 delitos sexuales sin

				contacto contra un menor. Además, el 86 % de todos los delitos sexuales sin contacto se cometieron en internet o utilizando herramientas informáticas.
Finlandia	2022	25 000	NCMEC y Save the Children	
Francia	1 de agosto de 2021 al 1 de agosto de 2022	120 000	NCMEC	
Alemania	-	-	-	Datos no disponibles / no comunicados
Grecia	2021 a 2022	142	NCMEC, línea directa griega para contenidos ilícitos en internet (Safeline), Comisión Nacional de Telecomunicaciones y Correos, línea nacional de SOS 1056 (The Smile of the child), Defensor del Pueblo griego	
Hungría	2022	0	Ninguna de las denuncias presentadas por proveedores se remitió en virtud del Reglamento provisional.	
Irlanda	2021 a 2022	15 355	NCMEC	
Italia	2022	4 607	No se especifica	
Letonia	1 de agosto de 2022 al 6 de marzo de 2023	Aproximadamente entre 115 y 220 denuncias mensuales	De proveedores y organizaciones no letones que actúan en interés público contra los abusos sexuales de menores (principalmente, el NCMEC) y de proveedores y organizaciones letones (principalmente, el Centro para un Internet más	

			Seguro de Letonia)	
Lituania	1 de enero de 2021 al 30 de junio de 2022	4 142	No se especifica	
Luxemburgo	2021 a 2022	2 491	No se especifica	
Malta	-	-	-	Datos no presentados/comunicados
Países Bajos	2021	36 537	Proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores	
Polonia	3 de agosto de 2021 al 3 de agosto de 2023	227	Proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores	Respecto al período comprendido entre el 3 de agosto de 2022 y el 3 de agosto de 2023, Polonia notificó 1 denuncia de captación de menores y 105 denuncias de MASM.
Portugal	-	-	-	Datos no presentados/comunicados
Rumanía	-	-	-	Datos no presentados/comunicados
Eslovaquia	1 de agosto de 2021 al 31 de julio de 2022	7 206	Proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores	
Eslovenia	1 de enero de 2021 al 14 de julio de 2023	452	Esta cifra indica los delitos relacionados con actividades en internet. En la actualidad, 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.	
España	2022	31 474	Organizaciones que actúan en interés público contra los abusos	

			sexuales de menores	
Suecia	Agosto de 2021 al 31 de diciembre de 2022	32 830	Principalmente, el NCMEC	

Dado que el NCMEC es la principal fuente de denuncias, es esclarecedor comparar las cifras de las denuncias recibidas por los Estados miembros con las indicadas por el NCMEC respecto a las denuncias remitidas a los Estados miembros. En 2021, el NCMEC recibió un total de 29 397 681 denuncias del sector a nivel mundial, de las cuales el 99,7 % (o 29 309 106) contenía una o varias imágenes o vídeos de abusos sexuales de menores, el 0,15 % (o 44 155) estaba relacionado con la captación de menores y el 0,05 % (o 16 032), con la trata de menores con fines sexuales. En 2022, el NCMEC recibió un total de 32 059 029 denuncias, de las cuales el 99,5 % (o 31 901 234) estaba relacionado con imágenes o vídeos de abusos sexuales de menores, el 0,25 % (80 524), con la captación de menores y el 0,06 % (o 18 336), con la trata de menores con fines sexuales. Por lo que respecta a la UE, el desglose es el siguiente:

Cuadro n.º 7: Denuncias del NCMEC de presuntos abusos sexuales de menores en línea remitidas a los Estados miembros de la UE en 2021 y 2022

País	Denuncias totales en 2021 ¹⁰	% del total de la UE en 2021	Denuncias totales en 2022 ¹¹	% del total de la UE en 2022	% de la población de la UE
Austria	7 580	1,36 %	18 501	1,23 %	2,00 %
Bélgica	15 762	2,84 %	50 255	3,34 %	2,60 %
Bulgaria	13 584	2,44 %	31 937	2,12 %	1,53 %
Croacia	4 744	0,85 %	11 693	0,78 %	0,86 %
Chipre	2 657	0,48 %	7 361	0,49 %	0,20 %
Chequia	15 004	2,70 %	61 994	4,12 %	2,36 %
Dinamarca	5 891	1,06 %	30 215	2,01 %	1,31 %
Estonia	2 729	0,49 %	6 408	0,43 %	0,30 %
Finlandia	6 079	1,09 %	10 904	0,73 %	1,24 %
Francia	98 233	17,67 %	227 465	15,13 %	15,16 %
Alemania	79 701	14,34 %	138 193	9,19 %	18,59 %
Grecia	14 616	2,63 %	43 345	2,88 %	2,37 %
Hungría	31 710	5,70 %	109 434	7,28 %	2,16 %
Irlanda	7 327	1,32 %	19 770	1,31 %	1,13 %
Italia	37 480	6,74 %	96 512	6,42 %	13,32 %
Letonia	1 537	0,28 %	3 688	0,25 %	0,42 %
Lituania	3 509	0,63 %	16 603	1,10 %	0,63 %
Luxemburgo	2 005	0,36 %	2 004	0,13 %	0,14 %
Malta	750	0,13 %	4 713	0,31 %	0,12 %
Países Bajos	36 790	6,62 %	57 012	3,79 %	3,96 %
Polonia	37 758	6,79 %	235 310	15,65 %	8,41 %
Portugal	34 415	6,19 %	42 674	2,84 %	2,31 %
Rumanía	32 765	5,89 %	96 287	6,40 %	4,25 %

¹⁰ NCMEC, [Informes por país de la CyberTipline de 2021](#), consultados en noviembre de 2023.

¹¹ NCMEC, [Informes por país de la CyberTipline de 2022](#), consultados en noviembre de 2023.

Eslovaquia	7 275	1,31 %	39 748	2,64 %	1,21 %
Eslovenia	3 162	0,57 %	14 795	0,98 %	0,47 %
España	33 136	5,96 %	77 727	5,17 %	10,60 %
Suecia	19 635	3,53 %	48 883	3,25 %	2,33 %
Total	555 834		1 503 431		

Las significativas disparidades entre el número de denuncias en 2021 y 2022, que muestran un acusado aumento de las denuncias en 2022, se deben en gran parte a la disminución de la detección voluntaria entre enero y agosto de 2021, cuando el Reglamento provisional aún no era aplicable.

En sus estadísticas por Estado miembro de la UE, el NCMEC no hace distinciones según la fuente de la denuncia, en concreto si estas procedían de un servicio de comunicaciones interpersonales independiente de la numeración. No obstante, este centro sí proporciona estadísticas sobre el número total de denuncias que incumben a la UE procedentes de servicios de comunicaciones interpersonales independientes de la numeración. En 2021, 283 265 denuncias que incumbían a los Estados miembros procedían de un servicio de chat, mensajería o correo electrónico, es decir, el 51 % del total de denuncias que incumbían a la UE. Otras 164 645 denuncias (30 % del total) procedían de redes sociales o plataformas de juegos en línea, que puede que llevaran incorporados también servicios de mensajería o chat. En 2021, 3 565 denuncias que incumbían a la UE tenían que ver con la captación de menores. En 2022, 1 015 231 denuncias que incumbían a los Estados miembros procedían de un servicio de chat, mensajería o correo electrónico, es decir, el 68 % del total de denuncias que incumbían a la UE. Otras 325 847 denuncias (22 % del total) procedían de redes sociales o plataformas de juegos en línea, que puede que llevaran incorporados también servicios de mensajería o chat. En 2022, 7 561 denuncias que incumbían a la UE tenían que ver con la captación de menores. Una vez más, las disparidades en el número de denuncias presentadas por los servicios de comunicaciones interpersonales independientes de la numeración en 2021 y 2022 se deben a la disminución de la detección voluntaria entre enero y agosto de 2021, cuando el Reglamento provisional aún no era aplicable.

En muchos casos, la proporción de denuncias por Estado miembro se corresponde a grandes rasgos con la proporción de población del Estado miembro frente a la población de la UE en su conjunto, lo que podría apuntar a una incidencia comparable de los abusos sexuales de menores en línea en todos los Estados miembros. Se observan desviaciones notables en relación con España e Italia, cuyos porcentajes de ambos años resultan bajos en comparación con el porcentaje de población de la UE, mientras que la proporción de denuncias que incumbían a otros Estados miembros al parecer fluctúa significativamente (p. ej., Alemania, Polonia, Países Bajos y Eslovaquia). Estos cambios no se reflejan como tales en los informes sobre el número de casos, por lo que, una vez más, es difícil extraer conclusiones sobre la correlación entre denuncias e investigaciones.

En vista de las diferencias entre los períodos de notificación, no es posible establecer una correspondencia directa, si bien existen notables disparidades entre las estadísticas facilitadas por

el NCMEC y las cifras comunicadas por los Estados miembros. Además, tampoco puede establecerse una correspondencia plena entre las cifras del NCMEC correspondientes a los Estados miembros y las facilitadas por el sector e indicadas en la sección anterior. Aunque algunas de las diferencias pueden deberse a las denuncias de abusos sexuales de menores en línea provenientes de fuentes distintas de las comunicaciones interpersonales, sería necesario un análisis en mayor profundidad, dado que también es posible que otros proveedores distintos de los que han presentado informes a la Comisión hasta la fecha estén aplicando medidas de detección voluntaria que incumban a la UE, habida cuenta de la lista de proveedores que presentan denuncias ante el NCMEC¹². No obstante, el hecho de que en la mayoría de los Estados miembros parezca existir una 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.

Por cada denuncia del NCMEC anteriormente indicada, las imágenes y vídeos asociados de abusos sexuales de menores se suprimieron y retiraron de la circulación. Esto es importante en particular para las víctimas actuales y los supervivientes de abusos sexuales de menores. Los estudios han demostrado que la circulación continuada de imágenes y vídeos en los que se muestren los abusos sufridos merma la capacidad de las víctimas de sobreponerse a los efectos psicológicos de los abusos y genera una forma secundaria de victimización.

2.2.2. Número de menores identificados

La mayoría de los Estados miembros facilitaron estadísticas completas o parciales sobre el número de menores identificados, desglosado por género, de conformidad con el artículo 8, apartado 1, letra b), del Reglamento provisional. No obstante, varios Estados miembros no aportaron ningún dato ni justificación por no haber presentado informes con arreglo a dicha disposición.

Varios Estados miembros solo facilitaron estadísticas parciales referentes al período de notificación o no facilitaron ninguna, pero adujeron los motivos de ello. Entre los motivos aducidos cabe citar los siguientes:

- los menores víctimas de ASM en línea no pueden contabilizarse (Francia);
- no hay datos disponibles, ya que no se recabaron en el marco de la recopilación nacional de datos estadísticos / las autoridades nacionales no registraron estas estadísticas (Dinamarca y Lituania);
- los datos no están desglosados por género en la recopilación nacional de datos estadísticos (Bélgica, Chequia, Chipre, Grecia, Irlanda, Italia, Lituania y Países Bajos);
- no se dispone de información con el nivel de detalle requerido en los sistemas de información existentes (Finlandia);
- la información no se recoge (Alemania).

¹² Los datos del NCMEC están disponibles [aquí](#).

Algunos de los Estados miembros que indicaron que no podían facilitar estadísticas confirmaron que se había solicitado a sus autoridades nacionales que modificaran su procedimiento de registro de denuncias voluntarias e investigaciones y de recopilación de estadísticas (Dinamarca), o que estaban implantando nuevos sistemas de información que permitirían previsiblemente presentar informes con el nivel de detalle requerido (Finlandia).

En un Estado miembro, los datos que figuran a continuación no hacen distinción entre menores víctimas de ASM en línea y fuera de línea (Hungría). En algunos casos, las estadísticas también incluyen a los menores que se constató que habían producido y cargado el material en cuestión por sí mismos (material autogenerado, en su mayoría vídeos) (Chequia y Estonia).

Dado que los Estados miembros facilitaron mayoritariamente datos correspondientes a distintos períodos de notificación, no fue posible calcular el número total de menores identificados en la UE como víctimas de abusos sexuales de menores por año o en el mismo período de notificación.

Cuadro n.º 8: Número de menores identificados, desglosado por género

País	Período de notificación	Femenino	Masculino	Total	Observaciones
Austria	2021 a 2022	11	6	17	
Bélgica	2021 a 2022	-	-	63	Datos desglosados por género no disponibles.
Bulgaria	2022	50	12	62	
Croacia	1 de enero de 2021 al 31 de octubre de 2022	20	0	20	
Chipre	2022	-	-	102	Datos desglosados por género no disponibles.
Chequia	2022	-	-	30	Datos desglosados por género no disponibles.
Dinamarca	-	-	-	-	Datos no disponibles.
Estonia	2021	6	12	18	
Finlandia	-	-	-	-	Datos no disponibles.
Francia	-	-	-	-	Datos no disponibles.
Alemania	-	-	-	-	Datos no disponibles.
Grecia	2021 a 2022	-	-	4	Datos desglosados por género no disponibles.
Hungría	2021 a 2022	379	47	426	Es imposible diferenciar entre víctimas de ASM en línea y fuera de línea. Solo se incluyen los niños

					menores de 16 años.
Irlanda	2021 a 2022	-	-	101	Los datos de 2021 (50 víctimas) no pueden desglosarse por género. Los datos de 2022 desglosados por género son: 25 niñas y 26 niños identificados.
Italia	2022	-	-	385	Datos desglosados por género no disponibles.
Letonia	1 de agosto de 2022 al 6 de marzo de 2023	1	-	1	
Lituania	-	-	-	-	Datos no disponibles.
Luxemburgo	2021 a 2022	0	0	0	
Malta	-	-	-	-	Datos no presentados/comunicados
Países Bajos	2021	-	-	222	Datos desglosados por género no disponibles.
Polonia	2022	2 368	487	3 014	En 2022, los datos del Sistema de Información de la Policía Nacional de Polonia proporcionan información sobre 3 014 víctimas de delitos relacionados con ASM (2 368 niñas, 487 niños, 159 casos en los que no se indica el género).
Portugal	-	-	-	-	Datos no presentados/comunicados
Rumanía	-	-	-	-	Datos no presentados/comunicados
Eslovaquia	Agosto de 2021 a julio de 2022	13	8	21	
Eslovenia	1 de enero de 2021 al 14 de julio de 2023	220	85	305	
España	2022	80	39	119	
Suecia	2022	8	4	12	
TOTAL DE TODOS LOS ESTADOS	1 de enero de 2021 al 6 de marzo de 2023	3 156	700	4 922	

MIEMBROS					
-----------------	--	--	--	--	--

Los datos anteriores están sujetos a una serie de salvedades adicionales. Los datos estadísticos disponibles no siempre permiten a los Estados miembros separar los datos sobre las víctimas identificadas a partir de una denuncia de un proveedor de los datos de aquellos casos en los que, por ejemplo, podría haber denunciado el delito la propia víctima u otra persona que la conociera o que detectara el delito (como menciona Eslovenia). Suecia indicó que los menores identificados a través de registros de chats también se incluyen en el informe, aunque las fotografías o los vídeos de los abusos no se hayan encontrado nunca o no se haya constatado que procedan de esa víctima en particular.

En general, los datos del cuadro n.º 8 no se corresponden necesariamente con las obligaciones de notificación del Reglamento provisional, que se refieren únicamente a las víctimas rescatadas gracias a las denuncias presentadas por proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores en virtud del Reglamento. En algunos casos, los datos facilitados incluyen a las víctimas identificadas por otros motivos y medios diversos.

Por lo tanto, los datos no permiten extraer una visión global del número de menores identificados en la UE como víctimas de abusos sexuales de menores en línea.

Además, aun cuando se haya identificado a una víctima, ello no implica necesariamente que se haya impuesto una condena vinculada a dicha identificación. En algunos casos, se identificó a la víctima, pero la investigación no logró dar con un sospechoso o no dio lugar a una condena (Suecia).

No obstante, de los datos puede inferirse que se ha identificado un número de víctimas significativo gracias a una denuncia voluntaria de conformidad con el Reglamento provisional. Así lo confirman los informes de casos de las autoridades policiales, los cuales a menudo solo se abren sobre la base de denuncias voluntarias¹³.

2.2.3. Número de infractores condenados

Aunque la mayoría de los Estados miembros cumplieron sus obligaciones, dos Estados miembros no facilitaron ningún dato o justificación por no haber presentado informes con arreglo al artículo 8, apartado 1, letra c), del Reglamento provisional.

Varios Estados miembros no facilitaron estadísticas referentes al período de notificación con arreglo a dicha disposición y adujeron los siguientes motivos:

- los datos no están disponibles aún (Bélgica y España);
- la base de datos central utilizada para registrar delitos no requería registrar la naturaleza de la remisión inicial (Irlanda);

¹³ Véase, por ejemplo, una lista de ejemplos de casos en toda la UE que se abrieron gracias a las denuncias voluntarias por parte de empresas en la [evaluación de impacto](#) que acompaña a la propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores (véase en particular el anexo 7).

- los datos no se recogen (Alemania).

Los Estados miembros comunicaron datos muy diversos sobre el número de infractores condenados y no había coherencia entre los períodos de notificación abarcados, como se muestra en el cuadro n.º 8 que figura a continuación.

Cuadro n.º 9: Número de infractores condenados

País	Período de notificación	Número de condenas	Observaciones
Austria	2021	850	Los datos no hacen distinción entre los delitos cometidos en línea y fuera de línea.
Bélgica	-	-	Datos no disponibles.
Bulgaria	2021 a 2022	52	
Croacia	-	-	Datos no disponibles.
Chipre	2022	0	No hay condenas hasta la fecha.
Chequia	1 de enero de 2022 al 31 de julio de 2022	20	
Dinamarca	2 de agosto de 2021 al 20 de enero de 2023	224	
Estonia	2021	2	Solo se incluyen las condenas resultantes de denuncias del NCMEC.
Finlandia	2021	240	
Francia	4 de agosto de 2021 al 3 de agosto de 2022	820	
Alemania	-	-	Datos no disponibles.
Grecia	2021 a 2022	62	
Hungría	2021 a 2022	126	
Irlanda	-	-	Datos no disponibles.
Italia	2021 a 2022	5 835	Los datos no hacen distinción entre los delitos cometidos en línea y fuera de línea.
Letonia	2021 a 2022	33	Los datos no hacen distinción entre los delitos cometidos en línea y fuera de línea.
Lituania	1 de enero de 2021 al 30 de junio de 2022	10	
Luxemburgo	2022	11	Los datos no hacen distinción entre los delitos cometidos en línea y fuera de línea.
Malta	-	-	Datos no presentados/comunicados
Países Bajos	2021	217	
Polonia	Segundo semestre de 2021 al primer	185 / 194 / 81	

	semestre de 2022 / 2022 / Primer semestre de 2023		
Portugal	-	-	Datos no presentados/comunicados
Rumanía	-	-	Datos no presentados/comunicados
Eslovaquia	2021	10	
Eslovenia	2021 a 2022	45	
España	2022	-	Datos no disponibles.
Suecia	2022	55	

Es importante señalar que el número de condenas no es igual al número de infractores condenados, ya que una persona puede ser condenada por uno o varios delitos de abuso sexual de menores en línea.

Además, las estadísticas sobre condenas notificadas para un determinado período no están necesariamente vinculadas a las denuncias recibidas en ese período dado (es decir, una condena de 2022 podría estar vinculada, por ejemplo, a una denuncia de 2021 o 2020, y una denuncia de 2022 podría no dar lugar a una condena hasta 2023 o más adelante). Varios Estados miembros destacaron explícitamente este hecho en sus informes (Irlanda, Luxemburgo y Suecia).

En algunos casos, no se recopilaron estadísticas sobre si las denuncias de actividades sospechosas (p. ej., a través del NCMEC) dieron lugar a condenas o, en otras palabras, si las condenas fueron consecuencia de la información facilitada por un proveedor o una organización pública (Austria y Letonia). Solo Estonia confirmó de forma explícita que las estadísticas reflejan únicamente las condenas resultantes de denuncias del NCMEC. También es posible que las denuncias condujeran a otros infractores investigados y condenados en el transcurso de las investigaciones (Austria).

Generalmente se presupone que el número de condenas notificado se refiere a los casos finalizados tras la resolución de un recurso presentado a través del sistema judicial. En un Estado miembro (Dinamarca), en el que las cifras se recopilan en función de la última resolución, estas no son definitivas, ya que las resoluciones podrían haberse recurrido posteriormente.

En algunos casos, los datos almacenados en los sistemas informáticos nacionales y notificados por los Estados miembros no distinguen entre delitos cometidos en línea y fuera de línea (Austria, Luxemburgo y Letonia).

Los informes tan diversos presentados por los Estados miembros y la forma en que los datos estadísticos se recopilan a nivel nacional no permiten, así pues, extraer una visión global del número de infractores condenados en la UE por abuso sexual de menores en línea. En la actualidad tampoco es posible, sobre la base de los datos disponibles, vincular claramente estas condenas con denuncias presentadas en períodos concretos de notificación por proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores con arreglo al Reglamento.

2.3. Avances tecnológicos

Entre las tecnologías utilizadas actualmente para detectar el abuso sexual de menores en línea se incluyen tecnologías y herramientas para detectar el MASM «conocido» (es decir, detectado anteriormente) y «nuevo» (es decir, no detectado anteriormente), así como el embaucamiento de menores (conocido como «captación de menores»).

En los ejemplos expuestos a continuación, figuran algunas de las herramientas más ampliamente utilizadas, que no conforman una lista exhaustiva. Muchas de estas herramientas se ponen a disposición de los proveedores, las autoridades policiales y otras organizaciones cuando puede demostrarse un interés legítimo. Normalmente, estas herramientas se combinan con la revisión humana para garantizar la máxima precisión posible.

En esta sección también se incluyen otros avances tecnológicos relacionados con la inteligencia artificial.

2.3.1. Detección de MASM conocido

Las tecnologías disponibles para detectar el MASM conocido se sustentan únicamente en el análisis automático de contenidos¹⁴ 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 (conocida como «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» ningún material que no se corresponda con el *hash* en cuestión. Además, los valores resumen no son reversibles y, por tanto, no pueden usarse para recrear una imagen.

Existen numerosas variaciones y aplicaciones de la tecnología de funciones de resumen. Entre las herramientas indicadas que se utilizan para las detecciones de MASM conocido, cabe citar las siguientes: i) [PhotoDNA de Microsoft](#); ii) [CSAI Match de Google](#); iii) [NeuralHash + Private Set Intersection de Apple](#); iv) [SSN++ de Meta](#); v) [PDQ y TMK+PDQF](#); vi) [generador de hashes MD5 \(Skype\)](#), y vii) [Safer \(Thorn\)](#).

La herramienta más ampliamente usada es PhotoDNA de Microsoft, utilizada por más de 150 organizaciones¹⁵. FotoDNA lleva más de diez años en uso y tiene un alto nivel de precisión. Se calcula que la tasa de falsos positivos no es superior a 1 entre 50 000 millones, según los ensayos¹⁶. La tasa de error de PhotoDNA se mantiene extremadamente baja debido a la naturaleza de esta tecnología. Esta detecta exclusivamente copias de contenidos previamente

¹⁴ Los proveedores no consideran que los metadatos sean una herramienta eficaz para detectar MASM. Véanse en particular las pp. 10 y 11 de Pfefferkorn, R., Stanford Internet Observatory, *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], 9 de septiembre de 2021.

¹⁵ Microsoft, [Unidad de Delitos Digitales](#).

¹⁶ [Testimonio de Hany Farid, desarrollador de PhotoDNA, ante la Comisión de Energía y Comercio sobre el fomento de un internet más sano para proteger a los consumidores, 16 de octubre de 2019.](#)

identificados. Mientras que la versión original de PhotoDNA detecta MASM conocido en imágenes, también está disponible una versión para detectar MASM en vídeos.

La tecnología se está desarrollando y 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. Además, la Internet Watch Foundation (IWF) informó recientemente de que había mejorado su tecnología de funciones de resumen¹⁷.

2.3.2. Detección de MASM nuevo

Entre las tecnologías utilizadas actualmente para la detección de MASM nuevo cabe citar los clasificadores y la inteligencia artificial (IA) que analizan imágenes y vídeos para detectar patrones de contenido que coincidan con patrones generados a partir del material de abuso sexual de menores anteriormente detectado. Un clasificador es un algoritmo que organiza los datos por clases o categorías de información etiquetadas a través del reconocimiento de patrones. Los clasificadores necesitan datos para su aprendizaje, y su precisión mejora a medida que se les alimenta con más datos.

Entre las herramientas para detectar MASM nuevo cabe citar las siguientes: i) [Safer](#) (Thorn); ii) [Content Safety API de Google](#); iii) tecnología de IA de Facebook¹⁸; iv) [Amazon Rekognition](#) y v) [Hive AI para contenidos visuales](#).

La investigación ha demostrado que las herramientas y los sistemas automatizados, como los clasificadores, son el medio más útil para detectar MASM¹⁹. En cuanto a la detección de MASM nuevo, el índice de precisión se sitúa actualmente 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 %²⁰. Es probable que estos parámetros mejoren a medida que aumenten su uso y retroalimentación.

¹⁷ Internet Watch Foundation (IWF), [Informe anual de 2022](#), pp. 129-133.

¹⁸ 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.

¹⁹ 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*, febrero de 2022, pp. 1-38.

²⁰ Thorn, [Thorn's Automated Tool to Remove Child Abuse Content at Scale Expands to More Platforms through AWS Marketplace](#) [«La herramienta automatizada de Thorn para retirar a gran escala contenido que representa abusos de menores se expande a más plataformas a través del mercado de AWS», disponible en inglés], 24 de mayo de 2021.

2.3.3. Detección de la captación de menores

Las herramientas para detectar la captación de menores (embaucamiento de menores) en comunicaciones basadas en texto utilizan tecnologías únicamente para detectar patrones que apunten a posibles elementos concretos de sospecha de abuso sexual de menores en línea, sin ser capaces de deducir el fondo del contenido. Esta técnica se aplica a las conversaciones de chat basadas en texto. Una serie de características de las conversaciones 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 sirven de determinante, establecido por cada empresa, para señalar aquellas conversaciones que deben ser objeto de una revisión humana adicional.

Entre las herramientas utilizadas en las operaciones de detección de texto cabe citar: i) el [Proyecto Artemis de Microsoft](#)²¹; ii) [Amazon Rekognition](#); iii) la tecnología [Spirit AI](#) de Twitch (basada en PLN y clasificadores de texto)²²; iv) el clasificador basado en el aprendizaje automático de clasificación desarrollado internamente por Meta (que combina tecnología de análisis interno del lenguaje con metadatos); v) el filtrado de chats de [Roblox](#)²³, y vi) la solución técnica de Thorn y Tech Coalition basada en el aprendizaje automático y los clasificadores²⁴.

Al igual que en el caso de la detección de MASM nuevo, la detección de contenido que implique la captación de menores requiere entrenar a la tecnología con este tipo de contenido. El acceso a esta clase de datos de entrenamiento sigue siendo el mayor obstáculo para el desarrollo y la mejora de estas tecnologías.

Thorn, en colaboración con Tech Coalition y sus miembros, ha puesto en marcha una nueva iniciativa encaminada a desarrollar una solución técnica para detectar y abordar los intentos de captación de menores en línea, que resultará útil y podrá utilizarse en una serie de plataformas que ofrecen comunicaciones basadas en texto. Se basará en el trabajo del equipo de Thorn en un clasificador basado en el PLN (procesamiento del lenguaje natural), o un modelo de aprendizaje automático, que detecta y categoriza el contenido o comportamiento en línea que encaja dentro de «clases» definidas relacionadas con la captación de menores (como la exposición a material sexual o el intento de concertar un encuentro en persona con un menor), además de asignar una

²¹ El Proyecto Artemis de Microsoft se desarrolló en colaboración con The Meet Group, Roblox, Kik y Thorn.

²² Para más información, véase: <https://safety.twitch.tv/s/article/Our-Work-to-Combat-Online-Grooming?language=es>.

²³ 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](#) [«Elementos de seguridad: chat, privacidad y filtrado», disponible en inglés], consultado en julio de 2023.

²⁴ Tech Coalition, [New Technology to Help Companies Keep Young People Safe](#) [«Nueva tecnología para ayudar a las empresas a mantener a salvo a los jóvenes», disponible en inglés], 20 de junio de 2023.

puntuación global del grado en que una conversación está relacionada con la captación de menores²⁵.

2.3.4. Nuevos retos planteados por los robots conversacionales y los generadores de arte o imágenes basados en la inteligencia artificial

El desarrollo y lanzamiento de robots conversacionales basados en IA como [ChatGPT](#) [un gran modelo de lenguaje (LLM, por sus siglas en inglés) desarrollado por [OpenAI](#)] y generadores de arte o imágenes como [DALL-E](#)²⁶ y [Midjourney](#)²⁷ ha despertado una gran atención entre el público, principalmente debido a su capacidad de facilitar respuestas listas para su uso y de crear imágenes realistas aplicables en un vasto número de diferentes contextos. Estas nuevas herramientas han adquirido rápidamente una popularidad y un uso generalizados. Los productos más destacados son financiados y desarrollados por empresas tecnológicas como Microsoft y Google, a la par que las nuevas tecnologías se están perfeccionando y se desarrollan versiones mejoradas periódicamente.

Si bien estas tecnologías ofrecen grandes oportunidades tanto a las empresas como a la ciudadanía, también pueden entrañar un riesgo para ellas. Entre las preocupaciones que suscitan estos productos se incluye la manera en que los delincuentes pueden querer utilizarlos para sus perversos objetivos, como la explotación sexual de menores.

Como ha informado Europol, si bien toda la información que proporciona ChatGPT está disponible libremente en internet, la herramienta hace que a los agentes malintencionados les resulte considerablemente más fácil aprender sobre un gran número de posibles ámbitos delictivos sin tener conocimientos previos, desde cómo allanar una morada hasta el terrorismo, la ciberdelincuencia y el abuso sexual de menores. Esto permite a dichas personas comprender mejor y, posteriormente, cometer este tipo de delitos²⁸.

Las normas de OpenAI restringen la capacidad de ChatGPT para responder a los comandos (*prompts*) orientados a generar contenido sexual, de odio, violento o que promueva la autolesión. No obstante, estas salvaguardias pueden eludirse con bastante facilidad mediante la ingeniería de comandos²⁹. El reciente lanzamiento de robots conversacionales basados en IA (p. ej., por

²⁵ Tech Coalition, [New Technology to Help Companies Keep Young People Safe](#) [«Nueva tecnología para ayudar a las empresas a mantener a salvo a los jóvenes», disponible en inglés], 20 de junio de 2023.

²⁶ DALL-E es un sistema de IA que puede crear imágenes realistas y arte a partir de una descripción en lenguaje natural.

²⁷ Midjourney es un programa y servicio generativo de inteligencia artificial que genera imágenes a partir de descripciones en lenguaje natural.

²⁸ Europol, [ChatGPT - The impact of Large Language Models on Law Enforcement](#) [«ChatGPT: el impacto de los grandes modelos de lenguaje en la aplicación de la ley», disponible en inglés], 2023, ISBN 978-92-95220-57-7, p. 7.

²⁹ Swanson, S. M., [ChatGPT Generated Child Sex Abuse When Asked to Write BDSM Scenarios](#) [«Chat GPT generó abusos sexuales de menores cuando se le pidió que escribiera escenarios de BDSM», disponible en inglés], *Vice*, 6 de marzo de 2023; Mitchell, A., [ChatGPT gives sick child sex abuse answer, breaking its rules](#) [«ChatGPT da una perturbadora respuesta que implica abuso sexual de menores, rompiendo así sus reglas»,

Snapchat) muestra cómo estos pueden saltarse los límites y generar interacciones ofensivas o peligrosas, que impliquen incluso abuso sexual de menores³⁰. Dado que ahora un mayor número de empresas está estudiando la posibilidad de probar robots conversacionales basados en IA en sus plataformas (Instagram, posiblemente WhatsApp, y Messenger), es preciso evaluar cuidadosamente su impacto en los usuarios, especialmente los niños y los jóvenes.

Estas nuevas herramientas también requieren las salvaguardias adecuadas a fin de que no se utilicen indebidamente para producir material de abuso sexual de menores ultrafalso generado por IA³¹. Al ritmo al que evolucionan las herramientas de IA, es probable que pronto sea mucho más fácil generar imágenes que no puedan distinguirse de las imágenes reales. Esta posibilidad plantea varios retos clave en la lucha contra los ASM, ya que la capacidad de las fuerzas y los cuerpos de seguridad para investigar y enjuiciar los casos de MASM e identificar a las verdaderas víctimas puede verse gravemente socavada si el MASM generado por ordenador sumamente realista se vuelve muy frecuente en internet³².

La investigación ha demostrado que el acceso a material de abuso sexual de menores suele ser el primer paso hacia los abusos físicos, independientemente de que el material represente abusos y explotación reales o de aspecto realista³³. Limitar la difusión de material de abuso sexual de menores ultrafalso generado por IA es, por tanto, crucial como forma de prevención en el lado de los infractores. Otra de las preocupaciones fundamentales es que los embaucadores de menores pueden utilizar las capacidades avanzadas de generación de texto de ChatGPT, en combinación con la IA de conversión de texto en imagen disponible gratuitamente, para generar con rapidez y facilidad contenido para perfiles falsos y conversaciones verosímiles con los jóvenes para captar a menores por internet. Si bien ChatGPT por sí mismo no alentaría a la gente a convertirse en embaucadores de menores en línea, sí permite que cualquiera alimente con tecnología de IA las conversaciones que mantenga con menores por internet para volverse más persuasivo y creíble de cara a sus víctimas, lo que propicia la manipulación³⁴. La IA generativa podría tener potencial

disponible en inglés], *New York Post*, 24 de julio de 2023; Europol, [ChatGPT - The impact of Large Language Models on Law Enforcement](#) [«ChatGPT: el impacto de los grandes modelos de lenguaje en la aplicación de la ley», disponible en inglés], 2023, ISBN 978-92-95220-57-7, p. 5.

³⁰ Fowler, G. A., [Snapchat tried to make a safe AI. It chats with me about booze and sex](#) [«Snapchat trató de crear una IA segura. Esta habla conmigo sobre alcohol y sexo», disponible en inglés], *The Washington Post*, 14 de marzo de 2023; Vincent, J., [Instagram is apparently testing an AI chatbot that lets you choose from 30 personalities](#) [«Instagram está probando al parecer un chatbot basado en IA que te deja escoger entre treinta personalidades», disponible en inglés], *The Verge*, 7 de julio de 2023.

³¹ Crawford, A., Smith, T., [Illegal trade in AI child sex abuse images exposed](#) [«Sale a la luz el comercio ilegal de imágenes de abusos sexuales de menores generadas por IA», disponible en inglés], BBC, 27 de junio de 2023.

³² Thiel, D., Stroebel, M., y Portnoff, R. (2023). [Generative ML and CSAM: Implications and Mitigations](#) [«Aprendizaje automático generativo y MASM: implicaciones y mitigaciones», disponible en inglés]. Stanford Digital Repository. Disponible en <https://purl.stanford.edu/jv206yg3793>. <https://doi.org/10.25740/jv206yg3793>. P. 2.

³³ Protect Children, [Protect Children's research in the dark web is revealing unprecedented data on CSAM users](#) [«La investigación de Protect Children en la red oscura está revelando datos sin precedentes sobre los usuarios de MASM», disponible en inglés], 6 de junio de 2021; RAINN, [¿Qué es Material de Abuso Sexual Infantil \(MASI\)?](#), 25 de agosto de 2022.

³⁴ Breck Foundation, [Is artificial intelligence putting children at risk?](#) [«¿Pone en peligro a los menores la inteligencia artificial?», disponible en inglés], 9 de febrero de 2023, actualizado el 3 de abril de 2023.

para contribuir a un aumento de los casos de captación de menores en línea e incluso para automatizar la captación de menores a gran escala³⁵.

3. CONCLUSIONES

Medidas de aplicación adoptadas por los proveedores

Los informes de los proveedores revelaron que estos han venido detectando y denunciando los abusos sexuales de menores en línea en virtud del Reglamento provisional utilizando diversas tecnologías y procesos de detección. Todos los proveedores informaron del envío de estas denuncias al NCMEC. En cuanto al tipo y el volumen de datos personales tratados por los proveedores, los informes mostraron una gran variedad de datos de tráfico recogidos y diversos niveles de granularidad de los volúmenes de datos tratados, lo que impide a la Comisión obtener datos unificados a escala de la UE sobre los proveedores respecto al período de notificación en cuestión (de julio de 2021 al 31 de enero de 2023).

Los proveedores no indicaron el número ni las tasas de errores (falsos positivos) de las diferentes tecnologías utilizadas desglosados por tecnología empleada, sino que señalaron que aplicaban un enfoque por niveles para la detección de ASM en línea complementado con la revisión humana. Al mismo tiempo, los proveedores aplicaron un amplio abanico de medidas y salvaguardias para limitar y reducir la tasa de error en su detección. Además, los proveedores informaron de que contaban con políticas de conservación de los datos y salvaguardias de protección de datos en vigor, definidas en sus políticas o declaraciones de confidencialidad y respaldadas por salvaguardias y medidas normalizadas del sector en materia de protección de datos.

Medidas de aplicación adoptadas por los Estados miembros

El Reglamento provisional también obliga a los Estados miembros (de conformidad con su artículo 8) a proporcionar estadísticas clave sobre los casos de abuso sexual de menores en línea detectados y denunciados ante sus autoridades policiales, el número de menores víctimas identificados y el número de infractores condenados. Dado que los Estados miembros facilitaron en su mayoría datos referentes a distintos períodos de notificación, no fue posible calcular a partir de los datos presentados el número total de denuncias recibidas de abusos sexuales de menores en línea detectados a escala de la UE. Además, las denuncias recibidas y notificadas por los Estados miembros podrían diferir de las denuncias susceptibles de ser objeto de medidas (es decir, las denuncias que podrían utilizarse para abrir investigaciones) o del número de casos notificado. Solo unos pocos Estados miembros indicaron el tipo de proveedores en cuyos servicios se habían detectado los abusos sexuales de menores en línea. En algunos casos, los datos estadísticos nacionales no diferencian entre los delitos investigados sobre la base de

³⁵ Butler, J., [AI tools could be used by predators to 'automate child grooming', eSafety commissioner warns](#) [«Las herramientas de IA podrían ser utilizadas por depredadores para “automatizar la captación de menores”, advierte la comisaria de eSafety», disponible en inglés], *The Guardian*, 19 de mayo de 2023.

denuncias presentadas por los proveedores y otras organizaciones que actúan en interés público contra los abusos sexuales de menores, y los delitos investigados sobre la base de otras denuncias.

En consecuencia, no fue posible extraer de los informes recibidos el número total de menores identificados como víctimas de abusos sexuales de menores en línea en la UE, desglosado por género. Entre los motivos de ello cabe citar, por ejemplo: la notificación de datos referentes a períodos distintos; el uso de límites de edad diferentes para definir a los menores víctimas de ASM en línea; la falta de recopilación de estadísticas con ese nivel de detalle a escala nacional debido a limitaciones técnicas o de otro tipo; la falta de distinción entre los menores víctimas de ASM en línea y fuera de línea, etc. Algunos Estados miembros incluyen también en sus estadísticas a los menores que habían producido material autogenerado y, lo que es más importante, a menudo las estadísticas no diferencian entre las víctimas identificadas a partir de las denuncias presentadas por proveedores y organizaciones que actúan en interés público contra los abusos sexuales de menores con arreglo al Reglamento, y las identificadas por otros motivos y medios.

La visión global del número de infractores condenados también es fragmentada. En algunos casos, estos datos no están disponibles, ya que en las bases de datos no se registró la fuente de la remisión inicial y, por tanto, los datos no distinguen entre los infractores condenados a raíz de denuncias presentadas con arreglo al Reglamento o por otras denuncias. En algunos casos, los datos almacenados en los sistemas informáticos nacionales tampoco distinguen entre delitos cometidos en línea y fuera de línea. Además, las estadísticas sobre condenas notificadas para un determinado período no están necesariamente vinculadas a las denuncias recibidas en ese período dado, sino que podrían estar relacionadas con denuncias de períodos anteriores. Las estadísticas recopiladas sobre el número de condenas también podrían diferir del número de infractores condenados (ya que un infractor podría tener varias condenas).

Así pues, las estadísticas heterogéneas presentadas por los Estados miembros, que al parecer no siempre recogen los datos de manera sistemática y adecuada, así como todos los factores mencionados, no permiten obtener una visión global de las denuncias recibidas de ASM en línea, del número de menores identificados como víctimas de este delito ni del número de infractores condenados a escala de la UE con arreglo al Reglamento. El hecho de que en la mayoría de los Estados miembros parezca existir una 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. Algunos Estados miembros confirmaron que sus autoridades competentes están siendo objeto de cambios estructurales o de reorganización asociados a la creación de nuevos departamentos responsables de investigar delitos relacionados con el abuso sexual de menores en línea. En algunos Estados miembros, también se están implantando nuevos sistemas informáticos y se ha pedido a las autoridades nacionales que modifiquen sus procedimientos de registro y sus estadísticas. Todo esto debería dar lugar a condiciones favorables para disponer de estadísticas más exactas de los Estados miembros en el futuro. En cualquier caso, la Comisión hará uso de sus competencias en virtud de los Tratados en la medida

necesaria para garantizar que los Estados miembros cumplan sus obligaciones de presentación de informes con arreglo al Reglamento provisional.

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 provisional, tanto por parte de los proveedores como de los Estados miembros. Una mayor normalización de los datos disponibles y su notificación, como los previstos en la propuesta de Reglamento para prevenir y combatir el abuso sexual de los menores³⁶, contribuiría a obtener una visión más completa de las actividades pertinentes en la lucha contra este delito. De lo anterior se desprende que es necesario que los proveedores y los Estados miembros realicen más esfuerzos para garantizar que la recogida y notificación de los datos se ajuste a los requisitos del Reglamento provisional.

Los datos disponibles revelan que, con el actual sistema voluntario de detección y denuncia, es posible que el material automáticamente señalado como posible MASM resulte no serlo tras una revisión humana. Esto puede deberse a la falta de un conjunto común de *hashes* y otros indicadores para detectar MASM confirmado como ilegal en la UE o a la existencia de normas jurídicas distintas en cada jurisdicción, en particular en la UE y los EE. UU., sobre todo en lo que respecta a las definiciones pertinentes. 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, en particular, sobre 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, la información facilitada indica que las tecnologías utilizadas corresponden a aplicaciones tecnológicas diseñadas con el único propósito de detectar y retirar el material de abuso sexual de menores en línea y denunciarlo ante las autoridades policiales y las organizaciones que actúan en interés público contra los abusos sexuales de menores. No se facilitó información sobre si la implantación de estas tecnologías se ajustaba al estado actual de la técnica y tenía lugar 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, la cuestión fundamental es si el Reglamento provisional logra el equilibrio que el legislador de la UE pretendía alcanzar entre, por un lado, 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 (dignidad, integridad, prohibición de un trato inhumano o degradante, vida privada y derechos del niño) y, por otro, la salvaguardia de los derechos fundamentales de los usuarios de los servicios contemplados (intimidad, protección de los datos

³⁶ 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](#)].

personales, libertad de expresión y tutela judicial efectiva). Los datos disponibles son insuficientes para extraer conclusiones definitivas a este respecto. 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.

A pesar de las deficiencias de los datos disponibles, que no permiten conocer el uso que se hace de las denuncias voluntarias en un significativo número de Estados miembros, de ellos se desprende claramente que, en el período de notificación, se identificó a miles de menores, se obtuvieron más de dos mil condenas y se retiraron millones de imágenes y vídeos de la circulación, lo que redujo la victimización secundaria. Por consiguiente, se puede concluir que la denuncia voluntaria ha contribuido significativamente a la protección de un gran número de menores, incluso frente a abusos continuados, y puede deducirse que el Reglamento provisional es eficaz.