

PREDICCIÓN DE EDAD EN CHATGPT Y EL MARCO REGULATORIO EUROPEO:

**Análisis de los desafíos jurídicos de la elaboración de perfiles
automatizada,
el Reglamento de Inteligencia Artificial (RIA) y el RGPD**

Dolores Abuin

Febrero de 2026

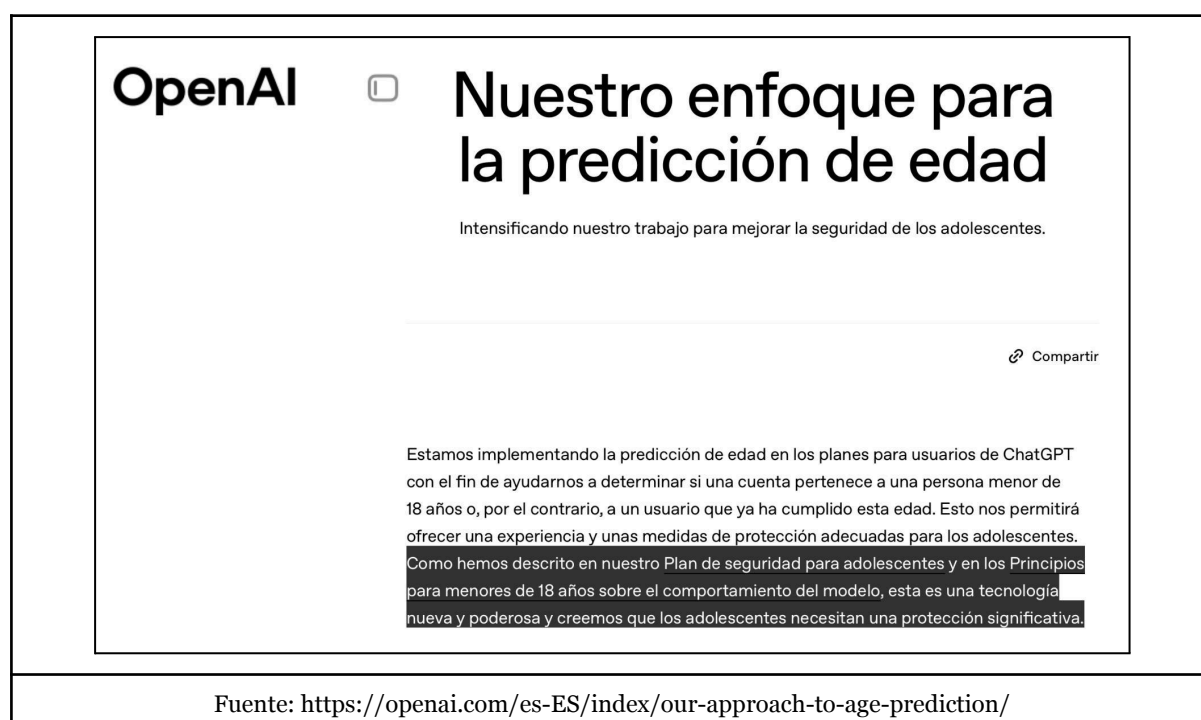
Palabras clave: predicción de edad, ChatGPT, Reglamento de Inteligencia Artificial, RGPD, elaboración de perfiles, social scoring, verificación biométrica, decisiones automatizadas, protección de menores, OpenAI

RESUMEN

En enero de 2026, OpenAI anunció globalmente un sistema de predicción de edad en ChatGPT que analiza patrones de comportamiento del usuario (horarios de uso, patrones de actividad, antigüedad de la cuenta) para inferir si eres menor de 18 años y aplicar restricciones automáticas. Cuando el sistema comete un error de clasificación, el único mecanismo de corrección disponible es una verificación biométrica gestionada por un tercero comercial (Persona). El presente trabajo analiza los desafíos jurídicos que esta funcionalidad genera bajo el Reglamento (UE) 2024/1689 de Inteligencia Artificial (RIA) y el Reglamento (UE) 2016/679 de Protección de Datos (RGPD). Se examina la proximidad del sistema con las prácticas prohibidas de *evaluación y clasificación a personas físicas* del artículo 5 del RIA, su probable clasificación como sistema de alto riesgo por la vía del perfilado (artículo 6.3) y la aplicabilidad del artículo 22 del RGPD sobre decisiones automatizadas. Se concluye que, aunque el objetivo de protección infantil es legítimo, el diseño específico del sistema plantea desafíos regulatorios significativos en el contexto europeo.

1. INTRODUCCIÓN

El 20 de enero de 2026, OpenAI activó a nivel global un sistema de predicción de edad para las cuentas de Free, Plus y Pro de ChatGPT.¹ Anunciado por Sam Altman el 16 de septiembre de 2025², el sistema representa el primer despliegue a gran escala de perfilado automatizado en una plataforma de IA generativa con el propósito declarado de proteger a los menores.



The image shows a screenshot of an OpenAI blog post. The header includes the OpenAI logo and the title "Nuestro enfoque para la predicción de edad". Below the title is a subtitle: "Intensificando nuestro trabajo para mejorar la seguridad de los adolescentes." There is a "Compartir" button with a share icon. The main text of the post reads: "Estamos implementando la predicción de edad en los planes para usuarios de ChatGPT con el fin de ayudarnos a determinar si una cuenta pertenece a una persona menor de 18 años o, por el contrario, a un usuario que ya ha cumplido esta edad. Esto nos permitirá ofrecer una experiencia y unas medidas de protección adecuadas para los adolescentes. Como hemos descrito en nuestro Plan de seguridad para adolescentes y en los Principios para menores de 18 años sobre el comportamiento del modelo, esta es una tecnología nueva y poderosa y creemos que los adolescentes necesitan una protección significativa." At the bottom of the screenshot, the source is cited as: "Fuente: <https://openai.com/es-ES/index/our-approach-to-age-prediction/>".

¹CNBC, "OpenAI is rolling out age prediction for ChatGPT consumer plans," 20 de enero de 2026. Disponible en: <https://www.cnbc.com/2026/01/20/open-ai-age-prediction-chatgpt.html>

²OpenAI, "Avanzamos hacia la predicción de edad" 16 de septiembre de 2025. Disponible en: <https://openai.com/es-ES/index/building-towards-age-prediction/>

En la UE, la predicción de edad se implementará más tarde debido a requisitos adicionales.

A diferencia de los mecanismos convencionales de verificación de edad, que solicitan documentos de identidad o recurren al reconocimiento facial, este sistema opera mediante lo que OpenAI denomina “predicción de edad”. Se trataría de una inferencia basada en el análisis de patrones de comportamiento del usuario a lo largo del tiempo.³

Lo define literalmente de esta forma la propia OpenAI:

ChatGPT utiliza señales vinculadas a tu cuenta para predecir tu edad. Puede incluir cosas como cómo y cuándo se usa tu cuenta y desde cuándo existe. Estas señales ayudan a predecir si es probable que alguien tenga más o menos de 18 años.

Cuando el modelo clasifica una cuenta como perteneciente a un menor de 18 años, aplica restricciones de contenido de forma automática, sin intervención humana. Para los adultos clasificados erróneamente, el único mecanismo de recurso es la verificación biométrica a través de Persona, un servicio de identidad de terceros.⁴

Esta funcionalidad, aplicada a los más de 800 millones de usuarios semanales de ChatGPT,⁵ se despliega en un momento de máxima expectación con el marco regulatorio europeo. Las prohibiciones del artículo 5 del Reglamento de Inteligencia Artificial (RIA) son aplicables desde el 2 de febrero de 2025,⁶ y el Comité Europeo de Protección de Datos (EDPB) presentó los Comentarios del EDPB sobre el borrador de directrices de la Comisión Europea para protección de menores bajo el DSA (publicados entre mayo-junio de 2025) desaconsejando explícitamente la estimación algorítmica de edad.⁷

227 The main difference between age estimation and age verification measures is the level of 228 accuracy. Whereas age verification provides certainty about the age of the user in principle 229 down to the day, age estimation provides an approximation of the user's age.	Commented [A13]: Another important difference is that, although age estimation is less precise than age verification, it may entail a higher degree of interference with users' fundamental rights to data protection, as it may entail large scale processing to profile users, with a view to determine the likelihood that they are minors. Therefore, we propose to generally discourage the use of algorithmic age estimation because of the current high rates of false positives and negatives, and the significant degree of interference with users' fundamental right to data protection.
230 6.1.2 Determining whether to put in place age assurance measures	Commented [A14]: See comment above on part 5.
231 Before deciding whether to put in place any age assurance method, providers of online 232 platforms accessible to minors should always conduct an assessment to determine whether 233 such a method is appropriate to ensure a high level of privacy, safety and security for 234 minors on their service and whether it is proportionate, or whether such a high level may 235 be achieved already by relying on other less far-reaching measures ⁽²⁷⁾ . In this regard, the 236 Commission is of the view that providers should also consider other measures set out in 237 other sections of these guidelines as an alternative to age assurance measures.	

Fuente: https://www.edpb.europa.eu/system/files/2025-06/edpb_comments_europeancommission_article_28_dsa_en.pdf

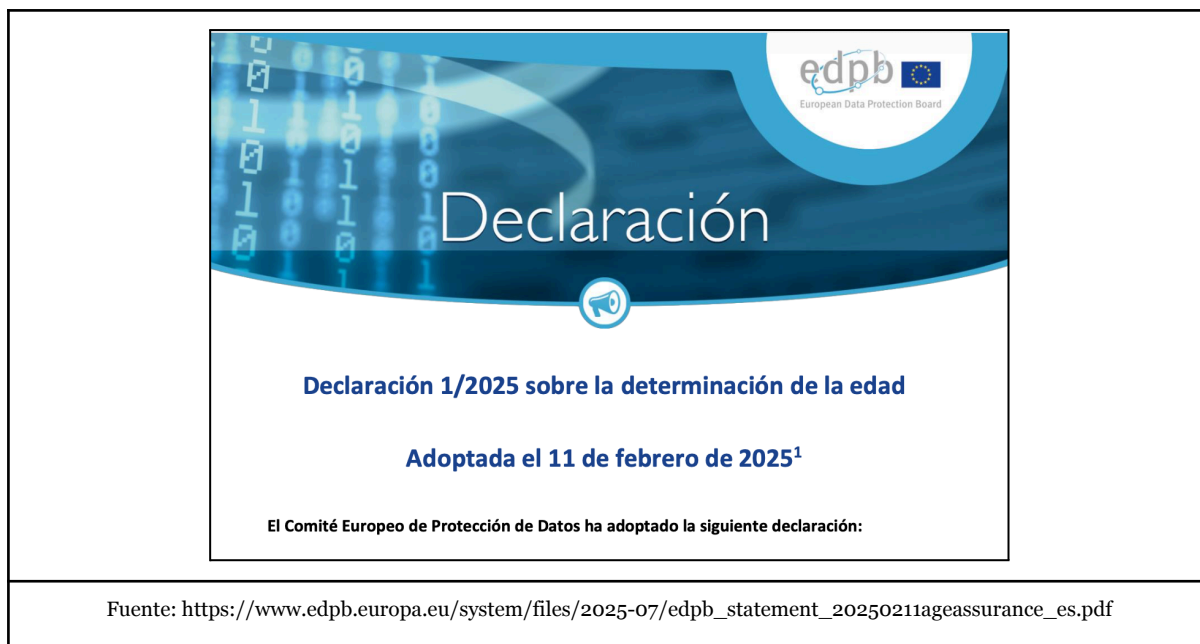
³OpenAI Help Center, “Age prediction in ChatGPT,” actualizado en febrero de 2026. Disponible en: <https://help.openai.com/en/articles/12652064-age-prediction-in-chatgpt>

⁴The Register, “OpenAI will try to guess your age before ChatGPT gets spicy,” 21 de enero de 2026. Disponible en: https://www.theregister.com/2026/01/21/openai_bets_on_age_prediction/

⁵ChatGPT alcanza 800 millones de usuarios semanales y domina el mercado de inteligencia generativa, 16 de febrero de 2026. Disponible en: <https://www.colglob.com/article/chatgpt-alcanza-800-millones-de-usuarios-semanales-y-domina-el-mercado-de-inteligencia-generativa-1771196766650>

⁶Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). DO L, 2024/1689, 12.7.2024.

⁷EDPB, Declaración 1/2025 sobre verificación de edad (Age Assurance), adoptada el 11 de febrero de 2025. Disponible en: https://www.edpb.europa.eu/system/files/2025-06/edpb_comments_europeancommission_article_28_dsa_en.pdf

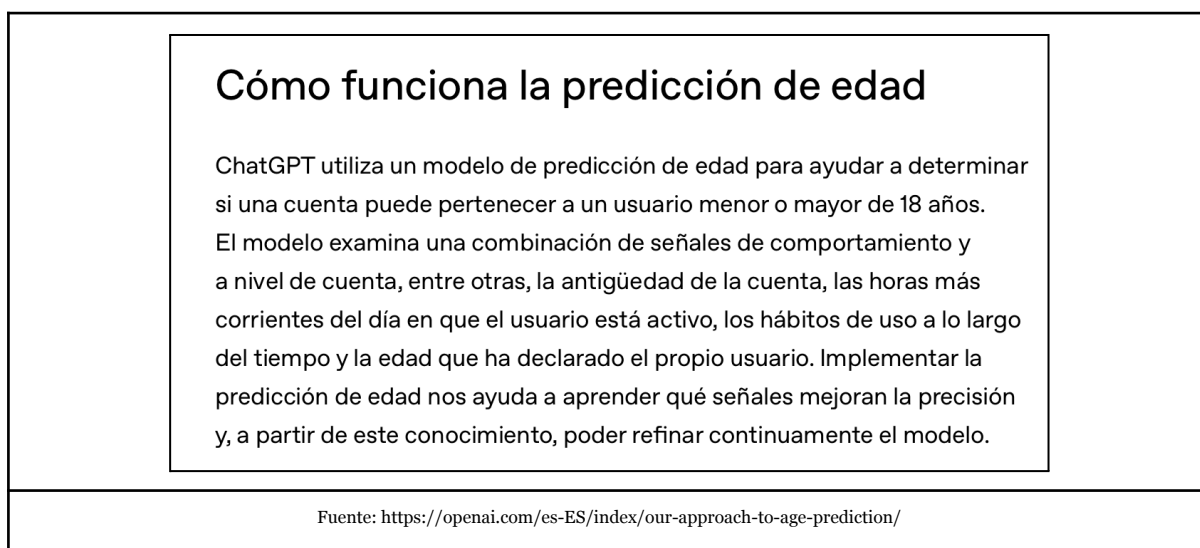


El presente trabajo analiza los desafíos legales entre el sistema de predicción de edad de ChatGPT y el marco normativo europeo, organizado en torno a varios ejes: (i) la clasificación del sistema bajo el RIA; (ii) su encaje en el régimen de decisiones automatizadas del RGPD; y (iii) la problemática específica de la relación de la predicción de la edad y los menores.

2. DESCRIPCIÓN TÉCNICA DEL SISTEMA

2.1. Señales de inferencia y mecanismo de clasificación

Según la documentación oficial de OpenAI, el sistema analiza cuatro tipos de señales: antigüedad de la cuenta, horarios típicos de actividad, patrones de uso a lo largo del tiempo y edad declarada por el usuario.⁸ Según OpenAI, “cuando no tenemos confianza sobre la edad de alguien o disponemos de información incompleta, optamos por una experiencia más segura”.⁹ Las cuentas nuevas con historial limitado pueden recibir automáticamente la configuración de adolescente.¹⁰



¹⁰Help Net Security, “OpenAI adds age prediction to ChatGPT to strengthen teen safety,” 21 de enero de 2026.

Las restricciones aplicadas incluyen el bloqueo de violencia gráfica, *roleplay* sexual o romántico, imágenes de autolesiones, contenidos que promuevan estándares de belleza extremos, dietas poco saludables o críticas corporales.¹¹ El sistema no incorpora al momento de realizar este estudio, mecanismos de supervisión humana previa a la aplicación de las restricciones, ni ha publicado métricas de precisión, ni tasa de falsos positivos o resultados de auditoría de sesgos.¹²

Cuando el modelo de predicción de edad determina que una cuenta puede pertenecer a un menor de 18 años, ChatGPT aplica automáticamente protecciones adicionales diseñadas para reducir la exposición a contenido sensible, entre ellas:

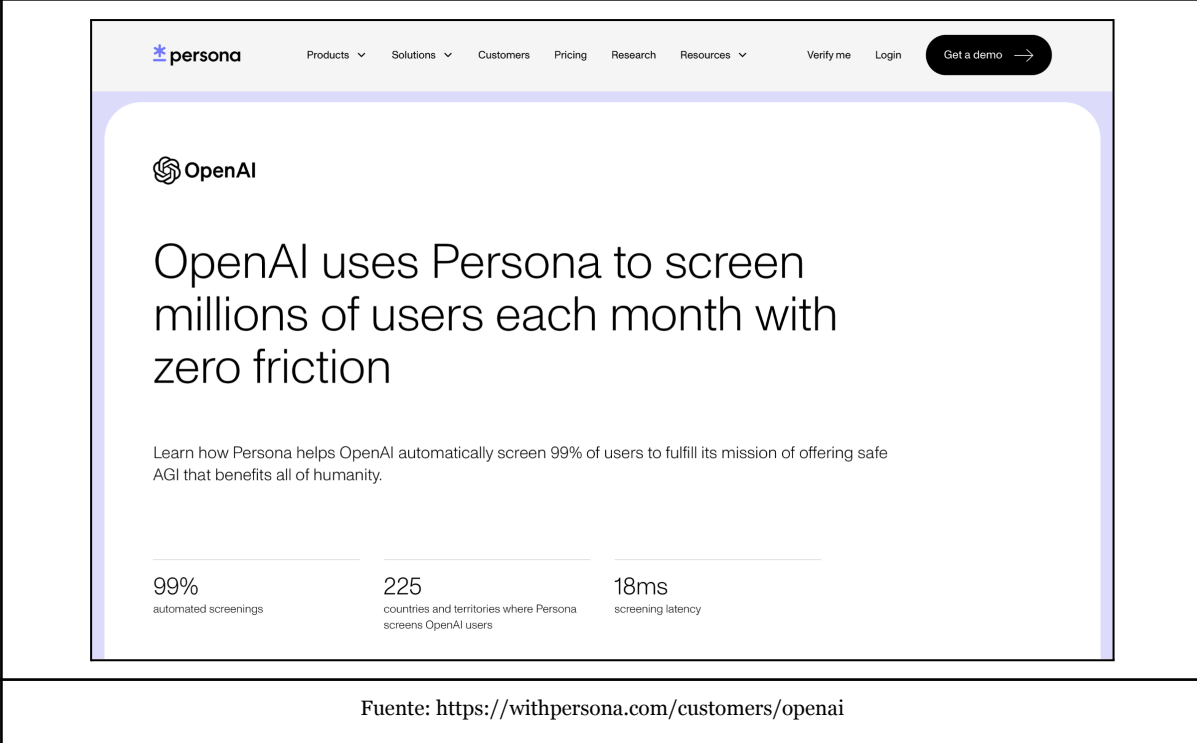
- Violencia gráfica o contenido sangriento
- Desafíos virales que pueden promover comportamientos arriesgados o perjudiciales en menores
- Juegos de roles sexuales, románticos o violentos
- Imágenes de autolesiones
- Contenido que promueve estándares de belleza extremos, dietas poco saludables o críticas corporales

Fuente: <https://openai.com/es-ES/index/our-approach-to-age-prediction/>

2.2. Mecanismo de rectificación: verificación biométrica por terceros

Para los adultos clasificados erróneamente, la única vía de corrección es la verificación a través de Persona, un servicio de identidad de terceros utilizado también por Coursera o WeTravel.¹³ El proceso requiere un *selfie* en vivo (teléfono o webcam) y, si este falla, un documento de identidad oficial (pasaporte, DNI, carnet de conducir). OpenAI afirma que solo recibe la confirmación de edad, no la imagen ni el documento.¹⁴ En Italia, los usuarios disponen de un plazo de 60 días para completar la verificación antes de que se desactiven determinadas funcionalidades.¹⁵

¹³Persona, “OpenAI Case Study.” Disponible en: <https://withpersona.com/customers/openai>



99%
automated screenings

225
countries and territories where Persona
screens OpenAI users

18ms
screening latency

Fuente: <https://withpersona.com/customers/openai>

3. ANÁLISIS BAJO EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

3.1. Artículo 5: Prácticas de IA prohibidas

El artículo 5, apartado 1, letra c), del Reglamento (UE) 2024/1689 prohíbe los sistemas de IA destinados a la evaluación o clasificación de personas físicas durante un período de tiempo, basándose en su comportamiento social o en características personales conocidas, inferidas o predichas, cuando dicha puntuación conduzca a un trato perjudicial que sea (i) injustificado o desproporcionado, o (ii) que se produzca en un contexto social no relacionado con el de la recogida de datos.¹⁶

El sistema de ChatGPT cumple formalmente algunos elementos de esta definición. Se clasifica a los usuarios en categorías (adulto/menor) y se basa en características inferidas a partir de patrones de comportamiento analizados a lo largo del tiempo. Sin embargo, las Directrices de la Comisión Europea publicadas el 4 de febrero de 2025 matizan el alcance de esta prohibición.¹⁷ El párrafo 175 de dichas Directrices aclara que no todas las prácticas de *social scoring* están prohibidas, sino solo aquellas que cumplan acumulativamente los criterios del artículo 5(1)(c).¹⁸ Además, el Considerando 31 del RIA permite la evaluación lícita de personas para un objetivo específico conforme al Derecho de la Unión.¹⁹

La protección infantil constituye un fin legítimo reconocido por el Derecho de la Unión y las restricciones se aplican en la misma plataforma donde se recogen los datos. No obstante, la proporcionalidad del artículo 5(1)(c)(ii) sigue siendo una zona gris. Si la tasa de falsos

¹⁶Artículo 5, apartado 1, letra c), del Reglamento (UE) 2024/1689.

¹⁷Comisión Europea, Directrices sobre prácticas prohibidas de IA (C 2025/884), publicadas el 4 de febrero de 2025.

¹⁸Privacy World, “The European Commission’s Guidance on Prohibited AI Practices: Unraveling the AI Act,” mayo de 2025.

¹⁹Considerando 31 del Reglamento (UE) 2024/1689.

positivos es elevada, si no existe supervisión humana antes de aplicar restricciones y si el mecanismo de recurso exige la entrega de datos biométricos a un tercero, el tratamiento quizá podría considerarse desproporcionado.

En cuanto a la categorización biométrica prohibida por el artículo 5(1)(g), la edad no figura entre las características protegidas de la lista exhaustiva (raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual).²⁰ Además, las señales que utiliza OpenAI (antigüedad de cuenta, horarios, patrones de uso) probablemente no constituyen “datos biométricos” según la definición del artículo 3(34), que se refiere a características físicas, fisiológicas o conductuales procesadas técnicamente para la identificación unívoca de una persona.²¹

3.2. Artículo 6(3): reglas de clasificación de los sistemas de IA de alto riesgo

El artículo 6, apartado 3, del RIA establece que los sistemas de IA incluidos en el Anexo III que realizan elaboración de perfiles (*profiling*) de personas físicas, según la definición del artículo 4.4 del RGPD, quedan automáticamente clasificados como alto riesgo, sin posibilidad de acogerse a la excepción de bajo riesgo.²² El sistema de ChatGPT infiere la edad a partir de datos personales (patrones de uso, contenido de conversaciones, datos de cuenta) para evaluar aspectos personales del usuario: esto constituye, textualmente, elaboración de perfiles.

Esta clasificación activaría todo el catálogo de obligaciones del Título III: sistema de gestión de riesgos (artículo 9), gobernanza de datos con *datasets* representativos y libres de errores (artículo 10), transparencia suficiente para que los usuarios comprendan el funcionamiento (artículo 13), vigilancia humana efectiva (artículo 14) y niveles adecuados de precisión y robustez (artículo 15).²³ Además, el artículo 26 exige a los responsables del despliegue realizar evaluaciones de impacto en derechos fundamentales y garantizar la vigilancia humana.²⁴ La aplicación automática de restricciones sin revisión humana previa podría infringir directamente el artículo 14.²⁵

Pero OpenAI nos añade una capa adicional a la verificación biométrica. Se trata de Persona, un sistema separado que sí procesa datos biométricos (análisis facial para verificación de identidad). Este componente podría clasificarse como categorización biométrica según el artículo 3(40) del RIA. El Considerando 16 menciona explícitamente la edad como categoría²⁶ y podría articularse bajo el Anexo III, punto 1(b), con las obligaciones reforzadas correspondientes, incluyendo la obligación de informar a los usuarios conforme al artículo 50(3).²⁷

²⁰Artículo 5, apartado 1, letra g), del Reglamento (UE) 2024/1689.

²¹Artículo 3, apartado 34, del Reglamento (UE) 2024/1689.

²²Artículo 6, apartado 3, del Reglamento (UE) 2024/1689, en relación con el artículo 4, apartado 4, del Reglamento (UE) 2016/679 (RGPD).

²³Artículos 9 a 15 del Reglamento (UE) 2024/1689 (Título III, Capítulo 2).

²⁴Artículo 26 del Reglamento (UE) 2024/1689: “Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo.”

²⁵Artículo 14 del Reglamento (UE) 2024/1689: “Vigilancia humana.”

²⁶Considerando 16 y artículo 3, apartado 40, del Reglamento (UE) 2024/1689.

²⁷Artículo 50, apartado 3, del Reglamento (UE) 2024/1689.

4. ANÁLISIS BAJO EL RGPD

4.1. Artículo 22: decisiones individuales automatizadas

El artículo 22, apartado 1, del RGPD establece que el interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o le afecte significativamente de modo similar.²⁸ La restricción automática del servicio por una clasificación algorítmica encaja plenamente en este supuesto. Se nos afecta al acceso a funcionalidades del servicio, nos modifica el comportamiento y las opciones del usuario y además esta situación persiste hasta que se completa una verificación biométrica. Las Directrices del Grupo de Trabajo del Artículo 29 (WP251rev.01) confirman que decisiones que influyen significativamente en las circunstancias, el comportamiento o las elecciones del individuo alcanzan el umbral del artículo 22.²⁹

Incluso si OpenAI invocase una excepción del artículo 22(2) (necesidad contractual, autorización legal o consentimiento explícito), el artículo 22(3) impone garantías mínimas inderogables. Se aludiría al derecho a obtener intervención humana, a expresar el punto de vista propio y a impugnar la decisión.³⁰ El hecho de ofrecer como único mecanismo de impugnación la entrega de datos biométricos a un tercero comercial no satisface estos requisitos.

4.2. La inversión de la carga de la prueba

El principio de exactitud del artículo 5(1)(d) del RGPD obliga al responsable del tratamiento a adoptar “todas las medidas razonables” para que los datos inexactos se rectifiquen sin dilación.³¹ El principio de responsabilidad proactiva del artículo 5(2) establece que la carga de demostrar el cumplimiento recae sobre el responsable, no sobre el interesado.³² Al exigir al usuario una verificación biométrica con un tercero para corregir un error de clasificación automatizada, OpenAI invierte esta carga de manera que diversos elementos del RGPD podrían prohibir:

En primer lugar, el artículo 12(2) del RGPD establece que el responsable “facilitará al interesado el ejercicio de sus derechos”. Según las directrices del EDPB, exigir verificaciones de identidad innecesarias constituye un incumplimiento de esta obligación de “facilitar”.³³

En segundo lugar, el artículo 16 otorga el derecho a obtener “sin dilación indebida”, la rectificación de datos inexactos. El hecho de condicionar este derecho a una verificación adicional con terceros plantea dudas sobre su compatibilidad con este precepto.³⁴

En tercer lugar, el principio de minimización de datos del artículo 5(1)(c) establece que los datos personales deben ser “adecuados, pertinentes y limitados a lo necesario”. Exigir datos biométricos (que el artículo 9 considera categoría especial

²⁸Artículo 22, apartado 1, del Reglamento (UE) 2016/679 (RGPD).

²⁹Grupo de Trabajo del Artículo 29, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 (WP251rev.01), adoptadas el 3 de octubre de 2017, revisadas el 6 de febrero de 2018.

³⁰Artículo 22, apartado 3, del Reglamento (UE) 2016/679.

³¹Artículo 5, apartado 1, letra d), del Reglamento (UE) 2016/679: principio de exactitud.

³²Artículo 5, apartado 2, del Reglamento (UE) 2016/679: principio de responsabilidad proactiva.

³³Artículo 12, apartado 2, del Reglamento (UE) 2016/679.

³⁴Artículo 16 del Reglamento (UE) 2016/679: derecho de rectificación.

con protección reforzada) para corregir un error de clasificación algorítmica puede considerarse un tratamiento excesivo respecto al fin perseguido.³⁵

Las Directrices 3/2019 del EDPB sobre videovigilancia subrayan la necesidad de alternativas menos intrusivas a datos biométricos cuando sea razonable (apartado 5).³⁶

5. POSICIONES DE LOS REGULADORES EUROPEOS

5.1. EDPB: Declaración 1/2025 sobre verificación de edad

La Declaración 1/2025 del EDPB, adoptada el 11 de febrero de 2025, constituye el documento de referencia más relevante.³⁷ La presidenta del EDPB, Anu Talus, declaró que los métodos de verificación de edad “deben ser lo menos intrusivos posible”.³⁸ La Declaración establece que la estimación algorítmica de edad implica un grado de interferencia más alto con los derechos fundamentales a la protección de datos que la verificación directa, ya que puede suponer un perfilado a gran escala. En sus comentarios sobre las directrices de la Comisión para la protección de menores bajo el Reglamento de Servicios Digitales (DSA), el EDPB desaconsejó con carácter general el uso de la estimación algorítmica de edad debido a las altas tasas de falsos positivos y negativos.³⁹

5.2. Autoridades nacionales: Garante italiano, CNIL y AEPD

El Garante italiano ha sido el regulador más agresivo en su actuación frente a OpenAI. La multa de 15 millones de euros de diciembre de 2024 incluyó, entre otras infracciones, la falta de un sistema adecuado de verificación de edad.⁴⁰ La CNIL francesa ha entendido que el sitio no debe conocer la identidad del usuario, y el verificador no debe saber qué sitios visita el usuario. Además, la CNIL ha señalado que tanto la recogida de datos biométricos en el sentido del artículo 9 del RGPD como el uso de sistemas que estimen la edad basándose en el historial de navegación son contrarios a las normas de protección de datos en este contexto.⁴¹ La AEPD española ha desarrollado un decálogo con un principio clave, la verificación debe orientarse a que los adultos demuestren su autorización, no a identificar a los menores, y además debe ser anónima para los proveedores de servicios.⁴²

³⁵Artículo 9 del Reglamento (UE) 2016/679: tratamiento de categorías especiales de datos personales.

³⁶Comité Europeo de Protección de Datos (EDPB), Directrices 3/2019 sobre el tratamiento de datos personales a través de dispositivos de vídeo, versión 2.0, adoptadas el 29 de enero de 2020.

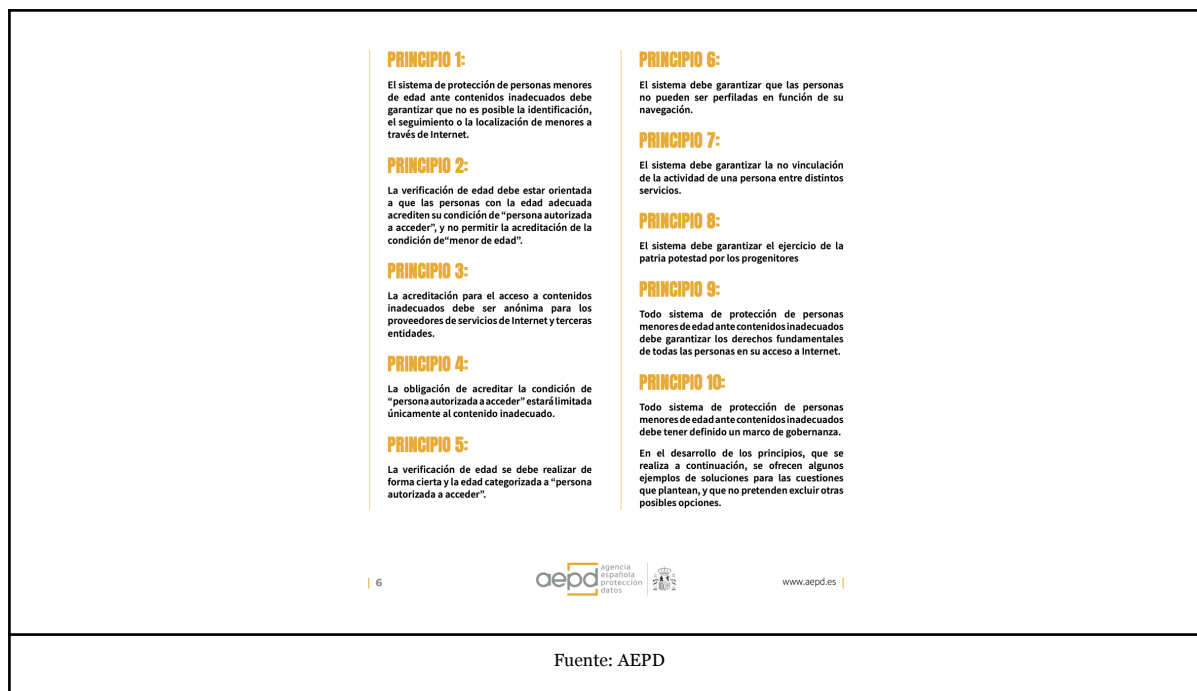
³⁸Declaraciones de la presidenta del EDPB, Anu Talus, en la sesión plenaria de febrero de 2025. Véase comunicado de prensa del EDPB de 12 de febrero de 2025.

³⁹EDPB, Comentarios sobre las directrices de la Comisión Europea relativas al artículo 28 del Reglamento de Servicios Digitales (DSA), junio de 2025.

⁴⁰Garante per la protezione dei dati personali, Provvedimento n. 755 del 2 de noviembre de 2024, publicado el 20 de diciembre de 2024. Véase PYMNTS, “Italian Authority Fines OpenAI \$15.6 Million for Alleged GDPR Violations,” 20 de diciembre de 2024.

⁴¹CNIL, “Online age verification: balancing privacy and the protection of minors,” 2024. Disponible en: <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>

⁴²AEPD, Sistema de verificación de edad para la protección de menores de edad, 2024.



Fuente: AEPD

5.3. Organizaciones de derechos digitales

Las reacciones de organizaciones de derechos digitales han sido especialmente críticas. Alexis Hancock (Electronic Frontier Foundation) ha señalado que el modelo no está obligado a ser correcto ni las decisiones pueden ser impugnadas de forma efectiva. Shirin Bhatia (Center for Democracy & Technology) ha advertido que predecir la edad basándose en estas señales es extremadamente difícil y que los primeros adoptantes de tecnología tienden a ser adolescentes, generando un sesgo estructural.⁴³ La organización noyb, liderada por Max Schrems, mantiene además una denuncia activa contra OpenAI por la incapacidad de ChatGPT para corregir datos personales inexactos conforme al artículo 16 del RGPD,^{44 45} un principio directamente aplicable al caso que nos ocupa.

6. CONCLUSIONES

El objetivo de proteger a los menores en plataformas de IA generativa es indiscutiblemente legítimo y urgente. Sin embargo, el diseño específico del sistema de predicción de edad de ChatGPT plantea un conflicto estructural con el marco regulatorio europeo.

Bajo el RIA, el sistema se sitúa en una zona gris del *social scoring* (artículo 5) pero probablemente calificaría como sistema de alto riesgo por la vía del perfilado (artículo 6.3), activando obligaciones que OpenAI debería estar cumpliendo.

Bajo el RGPD, la función encaja en el artículo 22 sobre decisiones automatizadas con efectos significativos, y la exigencia de verificación biométrica para rectificar un error automatizado constituye una probable inversión ilícita de la carga de la prueba bajo los principios de exactitud (artículo 5.1.d) y responsabilidad proactiva (artículo 5.2).

El EDPB ha desaconsejado expresamente la estimación algorítmica de edad,⁴⁶ y la CNIL ha considerado contrarios a las normas de protección de datos tanto la estimación basada en historial de navegación como la recogida de datos biométricos para verificación de edad.⁴⁷

⁴⁴noyb, Denuncia contra OpenAI por la incapacidad de ChatGPT para corregir datos personales inexactos conforme al artículo 16 del RGPD, 2024.

⁴⁵Infosecurity Magazine, "OpenAI's ChatGPT is Breaking GDPR, Says Noyb," 2024.

El retraso del despliegue europeo no ayuda en el mundo donde la IA y protección de datos, continuamente se cuestionan. La cuestión de fondo no es si debe protegerse a los menores (que debe hacerse), sino si un modelo opaco de posible perfilado masivo, sin métricas de precisión publicadas, sin supervisión humana y con un mecanismo de recurso que exige la entrega de datos biométricos a un tercero comercial para corregir errores de la máquina, constituye el enfoque adecuado bajo el Derecho europeo actual.

REFERENCIAS BIBLIOGRÁFICAS

Normativa europea

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial). *DO L*, 2024/1689, 12.7.2024.

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 (Reglamento General de Protección de Datos). *DO L* 119, 4.5.2016.

Comisión Europea, Directrices sobre prácticas prohibidas de IA (C 2025/884), 4 de febrero de 2025.

Documentos institucionales y de autoridades de protección de datos

EDPB, Declaración 1/2025 sobre verificación de edad (Age Assurance), adoptada el 11 de febrero de 2025.

EDPB, Comentarios sobre las directrices de la Comisión Europea relativas al artículo 28 del DSA, junio de 2025.

EDPB, Directrices 3/2019 sobre el tratamiento de datos personales a través de dispositivos de vídeo, versión 2.0, 29 de enero de 2020.

Grupo de Trabajo del Artículo 29, Directrices sobre decisiones individuales automatizadas y elaboración de perfiles (WP251rev.01), 3 de octubre de 2017, revisadas el 6 de febrero de 2018.

Garante per la protezione dei dati personali, Provvedimento correttivo e sanzionatorio nei confronti di OpenAI, provvedimento n.755 2024.

CNIL, “Online age verification: balancing privacy and the protection of minors,” 2024.

AEPD, Sistema de verificación de edad para la protección de menores de edad, 2024.

Fuentes primarias de OpenAI

OpenAI, “Our approach to age prediction,” 16 de septiembre de 2025.

OpenAI Help Center, “Age prediction in ChatGPT,” actualizado en febrero de 2026.

OpenAI, “Updating our Model Spec with teen protections,” 2025.

Prensa especializada y análisis

CNBC, “OpenAI is rolling out age prediction for ChatGPT consumer plans,” 20 de enero de 2026.

TechCrunch, “In an effort to protect young users, ChatGPT will now predict how old you are,” 20 de enero de 2026.

The Register, “OpenAI will try to guess your age before ChatGPT gets spicy,” 21 de enero de 2026.

Decrypt, “OpenAI Deploys Age Prediction to Restrict Teen Access on ChatGPT,” 21 de enero de 2026.

Help Net Security, “OpenAI adds age prediction to ChatGPT to strengthen teen safety,” 21 de enero de 2026.

Infosecurity Magazine, “OpenAI’s ChatGPT is Breaking GDPR, Says Noyb,” 2024.

Análisis jurídicos

Norton Rose Fulbright, “Prohibited practices under the AI Act: Answered and unanswered questions in the Commission’s guidelines,” marzo de 2025.

Privacy World, “The European Commission’s Guidance on Prohibited AI Practices: Unraveling the AI Act,” mayo de 2025.

William Fry, “The Time to (AI) Act is Now: A Practical Guide to Biometric Categorisation Systems Under The AI Act,” 2025.

DSA Observatory, “The Commission’s approach to age assurance: Do the DSA Guidelines on protecting minors online strike the right balance?,” julio de 2025.

IAPP, “Age verification and data protection: Far more difficult than it looks,” 2025.