

Seguridad infantil en línea

PROTEGER Y EMPODERAR
A LOS MENORES EN UN MUNDO DIGITAL

INFORME DE LOS COPRESIDENTES DEL GRUPO ESPECIAL

SOBRE SEGURIDAD INFANTIL EN LÍNEA

Prof. Dr. Jörg M. Fegert y Dr.^a Maria Melchior



El presente documento no debe considerarse representativo de la posición oficial de la Comisión Europea.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2026

© Unión Europea, 2026



La política de reutilización de la Comisión se aplica en virtud de la Decisión 2011/833/UE de la Comisión, de 12 de diciembre de 2011 relativa a la reutilización de los documentos de la Comisión (DO L 330 de 14.12.2011, p. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). Salvo que se indique otra cosa, se permite la reutilización de este documento conforme a la licencia Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). Esto significa que se permite la reutilización siempre que se señale adecuadamente la fuente y se indique cualquier cambio realizado.

Para cualquier uso o reproducción de elementos que no sean propiedad de la Unión Europea, puede ser necesario solicitar permiso directamente a los respectivos titulares de derechos.

Índice

PRÓLOGO

→ 04

PREFACIO

Crecer de forma segura en el mundo de los medios sociales+

→ 07

CAPÍTULO 1

Un enfoque de la seguridad infantil en línea basado en el desarrollo

→ 33

CAPÍTULO 2

Pruebas sobre los riesgos a los que se enfrentan los menores en línea

→ 60

CAPÍTULO 3

Protección de los menores en un entorno de medios sociales y otros servicios digitales en rápida evolución

→ 87

CAPÍTULO 4

Capacitar a los menores para navegar con seguridad por el mundo digital

→ 131

AGRADECIMIENTOS

→ 156

Prólogo

En marzo de 2026, la presidenta de la Comisión Europea, Ursula von der Leyen, encargó a dos consejeros especiales (Jörg M. Fegert y Maria Melchior) la copresidencia del Grupo Especial sobre Seguridad Infantil en Línea y posibles restricciones por edad en los medios sociales. Se encargó a los copresidentes que redactaran un informe sobre las conclusiones del Grupo y que asesoraran sobre el mejor enfoque para que Europa haga que el mundo digital sea más seguro para los niños.

El Grupo, anunciado por primera vez en el discurso sobre el estado de la Unión de 2025 por la presidenta de la Comisión, reunió a académicos de alto nivel, profesionales, representantes de jóvenes y padres y otros especialistas en diversos ámbitos de toda Europa para evaluar el impacto de los medios sociales en los menores.

Discurso sobre el estado de la Unión de 2025

El Grupo Especial se reunió en tres ocasiones y contó con la participación de diversos especialistas en cada ocasión. La primera reunión del Grupo tuvo lugar el 5 de marzo de 2026 y examinó las pruebas científicas existentes sobre el impacto de los medios sociales y, más en general, del entorno digital, en los niños y adolescentes.

La segunda reunión tuvo lugar el 16 de abril de 2026 y debatió la legislación y las herramientas vigentes de la UE, así como los enfoques políticos nacionales para abordar la seguridad infantil en línea. En su tercera reunión, el 16 de junio de 2026, el Grupo se centró en los enfoques políticos nacionales y las posibles recomendaciones para proteger y empoderar a los niños y adolescentes en el mundo digital.

**«Y, en esta labor,
nos guiaremos por
la necesidad de
empoderar a los padres
y de construir una
Europa más segura
para nuestros hijos.
Porque, cuando se
trata de la seguridad
de nuestros hijos
en el mundo digital,
Europa cree en los
padres, no en los
beneficios.»**

— URSULA VON DER LEYEN,
PRESIDENTA DE LA COMISIÓN EUROPEA

LOS PRINCIPALES TEMAS DEBATIDOS DURANTE

LAS REUNIONES FUERON LOS SIGUIENTES:

- // Los aspectos positivos y negativos de introducir restricciones específicas por edad para los medios sociales y otros servicios digitales;
- // Enfoques adaptados para proteger y empoderar a los menores en función de sus grupos de edad, el contexto socioeconómico y los riesgos específicos de cada edad;
- // La seguridad desde el diseño y por defecto y la responsabilidad de los proveedores de medios sociales y otros servicios digitales;
- // Medidas educativas y de sensibilización para promover un uso responsable de internet entre niños y adolescentes, padres y cuidadores, profesores y educadores;
- // Formas de apoyar a los padres y educadores y de capacitar a los niños y adolescentes para aprovechar las oportunidades del mundo digital.

El análisis y las recomendaciones del presente informe se basan en contribuciones cruciales de un grupo diverso de especialistas invitados a cada reunión del Grupo y en numerosas reuniones adicionales con representantes de los Estados miembros, en particular las organizadas por la Presidencia irlandesa del Consejo de la UE y Luxemburgo (reunión ministerial D9+), terceros países (incluidos Australia y Brasil), el Parlamento Europeo y sus diputados, especialmente del Intergrupo sobre los Derechos del Niño; la industria, la sociedad civil, los grupos de reflexión y otras organizaciones, como la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y el Comité Europeo de Protección de Datos (CEPD).

Tras estas interacciones y sobre la base de las pruebas recopiladas, los copresidentes elaboraron sus recomendaciones. Si bien la responsabilidad de las recomendaciones recae exclusivamente en los copresidentes, su trabajo se debe en gran medida a las aportaciones de otros expertos de renombre, representantes de padres y jóvenes, y a los conocimientos especializados proporcionados por la Comisión Europea.

El informe tiene por objeto servir de base para futuras acciones que propondrán la Comisión Europea y los Estados miembros de la UE para reforzar la seguridad infantil en línea. Esta evaluación analítica independiente ofrece recomendaciones e inspiración a los niños y adolescentes, los padres y cuidadores, los profesores y educadores, los proveedores de medios sociales y otros servicios digitales sobre cómo proteger y empoderar mejor a los menores en línea.

ÁMBITO Y TERMINOLOGÍA

La principal tarea, prescrita por la presidenta Von der Leyen, era que el Grupo Especial debatiera sobre la seguridad infantil en línea y las posibles restricciones por edad en los medios sociales. Si bien el ámbito del presente informe se ajusta a esta tarea, la evolución de los debates durante las reuniones del Grupo Especial y otros acontecimientos políticos (por ejemplo, el Llamamiento de los dirigentes del G7 sobre un espacio digital más seguro para los menores, de 17 de junio de 2026) subrayan la necesidad de que los copresidentes precisen la terminología utilizada en el presente informe.

Sin perjuicio de los actos jurídicos internacionales, de la UE o nacionales, a lo largo del presente informe se utilizan los siguientes términos y definiciones correspondientes:

Medios sociales y otros servicios digitales (abreviado, medios sociales+)

dentro del ámbito de aplicación del presente informe, los términos «medios sociales+» y «medios sociales y otros servicios digitales» se utilizan para definir de manera amplia los servicios que pueden estar disponibles para los menores y presentar características o contenido inapropiados para su edad o que entrañan riesgos (por ejemplo, características adictivas y perjudiciales, entre las que se incluyen el desplazamiento infinito por la pantalla, la reproducción automática, los algoritmos de recomendación y las notificaciones persistentes). Entre los proveedores de medios sociales y otros servicios digitales se encuentran las plataformas digitales que actúan como intermediarios de contenidos de terceros, como las redes sociales, y las tiendas de aplicaciones. También se incluyen los sistemas de IA que plantean riesgos para la seguridad y el desarrollo de los menores, incluidos los compañeros de IA, los videojuegos que exponen a los menores a prácticas comerciales perjudiciales o contactos peligrosos, y las plataformas de intercambio de vídeos que permiten un acceso inapropiado para la edad de los menores.

Menores, niños y adolescentes

sin perjuicio del uso legalmente definido del término «niños» (por ejemplo, en la Convención de las Naciones Unidas sobre los Derechos del Niño), este informe aboga por la necesidad de un enfoque centrado en el desarrollo para proteger a los menores en línea, que aborde los riesgos y vulnerabilidades específicos a los que están expuestos a diferentes edades. A efectos de este análisis, los autores utilizan el término «menores» para referirse a todos los niños y adolescentes menores de 18 años (la mayoría de edad). El término «adolescentes» se aplica a todos los menores de 13 a 18 años. El término «niños» se refiere a todos los menores de 13 años. El presente informe utiliza el término «derechos del niño» para referirse a los derechos de todos los niños y adolescentes menores de 18 años, tal como se definen en los textos jurídicos. El término «seguridad infantil en línea», tal como se indica en el mandato del proceso del panel especial, se utiliza como término genérico para la protección y el empoderamiento de los menores en el mundo digital.

PREFACIO

Crecer de forma segura en el mundo de los medios sociales+

El rápido avance de las tecnologías digitales ha cambiado radicalmente la forma en que los niños y adolescentes crecen e interactúan con sus iguales, padres, profesores y el mundo que los rodea. Al mismo tiempo, las actividades en el mundo fuera de línea siguen siendo cruciales para el aprendizaje, fomentando relaciones y experiencias significativas que conforman el desarrollo de los menores.

El mundo de los medios sociales+ ofrece muchas oportunidades para que los niños y adolescentes aprendan, establezcan conexiones, participen y sean creativos. Sin embargo, es necesario educar y capacitar a los menores para que aprovechen estas oportunidades y desarrollen todo su potencial.

A pesar de ello, **los espacios de los medios sociales+ también presentan una serie de riesgos** para el desarrollo saludable y el bienestar de los menores. Entre ellos se incluyen los riesgos de uso excesivo debido a características adictivas, la sustitución de actividades favorables al desarrollo, la exposición a contenidos perjudiciales y los contactos inapropiados en línea. Estos riesgos se ven amplificados por la aparición de nuevas tecnologías y requieren decisiones atrevidas, pero cuidadosas, para proteger a los niños y adolescentes en línea.

La adopción generalizada de los medios sociales y otros servicios digitales ha llevado a **los responsables políticos y los padres a una extrema preocupación por las amenazas a las que se enfrentan los niños y adolescentes en línea**. Si bien las restricciones por edad para el acceso a los medios sociales y otros servicios digitales han sido objeto de críticas, **pueden ser un paso preventivo necesario** hasta que se demuestre que los niños y adolescentes pueden acceder de modo seguro a los espacios de medios sociales+ o hasta que surjan alternativas seguras.

Las restricciones por edad no consisten en hacer que los padres y cuidadores o los propios niños y adolescentes sean los principales responsables de la seguridad de los menores en el mundo digital. Tampoco se trata de dejar que los proveedores se libren de esta responsabilidad. **Los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de la seguridad de los servicios que desarrollan y prestan.**

La carga de la prueba debe recaer en los proveedores, no en las autoridades reguladoras, los padres y los niños. **Hasta que demuestren que sus servicios son seguros desde el diseño, los proveedores de medios sociales y otros servicios digitales deben restringir el acceso a los menores de 13 años**

en la UE. Además de las restricciones a escala de la UE, los Estados miembros pueden introducir otras restricciones preventivas por edad para los adolescentes mayores de 13 años.

Las restricciones preventivas por edad son medidas inmediatas para alcanzar el objetivo a largo plazo de garantizar que los espacios de los medios sociales+ sean seguros para los menores mediante la promoción del cambio cultural. Los primeros resultados de los países que han introducido prohibiciones generales por edad para acceder a los medios sociales muestran que la mayoría de los menores encuentran la manera de eludir estas políticas. Al mismo tiempo, algunos menores se han apartado de los medios sociales y otros servicios digitales de riesgo y ahora disponen de más tiempo para actividades fuera de línea (como el deporte y las interacciones sociales en persona). Esto demuestra que el cambio progresivo en torno a las normas de uso de los medios sociales+ por parte de los menores no solo es posible sino que debe reconocerse.

Sin embargo, todo cambio lleva tiempo. Por ejemplo, la evolución de las actitudes sociales con respecto a la prohibición legislativa del castigo corporal en la educación llevó más de una generación (en concreto, en Alemania y Suecia). La prohibición del castigo corporal aclaró las expectativas de los padres, cuidadores, profesores y educadores, y mejoró la participación de los transeúntes para garantizar una educación de los menores sin violencia. El éxito de esta medida se ha demostrado con las tendencias positivas y mediante una evaluación constante desde su introducción.

La eficacia de las restricciones por edad también requeriría un cambio de actitud social. La evaluación continua y el seguimiento a largo plazo pueden ayudar a los responsables políticos a comprender si los hábitos de los menores y sus padres, cuidadores y educadores cambiarán con el tiempo.

Al crecer en el mundo actual de los medios sociales+, los niños y adolescentes deben poder llevar una vida sana y satisfactoria y aprovechar las oportunidades que ofrecen los medios sociales y otros servicios digitales. **Los derechos de los niños son de aplicación tanto en el mundo digital como en el mundo real,** desde el derecho a estar seguros y protegidos de la explotación económica y la delincuencia en todas sus formas (en particular, la violencia sexual) hasta el derecho a acceder a la información, la educación y el ocio.

Los niños tienen derecho a crecer en un entorno seguro que favorezca su desarrollo, tanto en el mundo digital como en el mundo real. Si bien debe mantenerse el apoyo a los menores en el mundo real, también debemos reconocer que los entornos digitales se han convertido en una parte cada vez más importante de su vida cotidiana. Por esta razón debe garantizarse su protección por defecto en todos los medios sociales y otros servicios digitales.

Los derechos de los niños deben sustentar las medidas de seguridad infantil en línea. Las posibles

«Durante décadas hemos hecho que el mundo real sea más seguro para los niños y debemos hacer lo mismo en el mundo digital. Las oportunidades positivas que ofrece la tecnología no pueden ir en detrimento de su seguridad, salud o felicidad.»

— URSULA VON DER LEYEN,
PRESIDENTA DE LA COMISIÓN EUROPEA

restricciones por edad deben respetar plenamente los derechos de los menores y ser proporcionadas y equilibradas con el interés superior del menor. Los medios utilizados para lograrlo deben seguir el ritmo de los avances tecnológicos.

Si bien los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de la seguridad de sus servicios, especialmente en el caso de los menores, **es necesario un ecosistema de agentes para proteger y empoderar a los niños y adolescentes en el entorno de los medios sociales+**. Desde las autoridades reguladoras que deben adoptar las medidas necesarias, hasta los proveedores que ofrecen servicios seguros y adaptados a la edad, pasando por los padres, cuidadores, profesores y educadores, que desempeñan un papel clave a la hora de supervisar y orientar las actividades en línea de los menores. A medida que los menores maduran y los entornos de los medios sociales+ cambian rápidamente, **el éxito del ecosistema depende de las acciones interconectadas de todos los agentes** compartiendo el mismo objetivo: niños y adolescentes creciendo de forma segura en un mundo digital.

Gráfico 1: Ecosistema para proteger y empoderar a los menores en línea



Aumento del impulso político para reforzar la seguridad infantil en línea

Durante los últimos meses se ha demostrado que la seguridad infantil en línea se está convirtiendo en una prioridad política en todo el mundo. La **introducción, aplicación y evaluación continua de un «retraso en el acceso a los medios sociales» por parte de Australia ha brindado enseñanzas clave al resto del mundo**. Otros países, como el Reino Unido y Canadá, han seguido su ejemplo con propuestas legislativas previstas, mientras que Indonesia ya ha adoptado una prohibición.

Un informe reciente sugiere que el 92 % de los europeos opina que reforzar la protección de los niños y adolescentes en el espacio digital debería ser una prioridad para la UE^a.

Los líderes europeos también han empezado a abordar la cuestión. La Declaración de Jutlandia^b de septiembre de 2025 y la Resolución del Parlamento Europeo en la que se pide una edad mínima digital armonizada a escala de la UE^c, la creación por la presidenta Von der Leyen del Grupo Especial sobre Seguridad Infantil en Línea, y las conclusiones recientes del Consejo Europeo^d, son indicaciones claras de que existe un creciente ímpetu político por adoptar medidas concretas para abordar los riesgos cada vez mayores a los que se enfrentan los niños en el mundo digital.

En junio de 2026, por primera vez, el G7 —que incluye a Canadá, Francia, Alemania, Italia, Japón, el Reino Unido, los Estados Unidos y la Unión Europea— acordó al más alto nivel político principios comunes para proteger a los menores de los servicios digitales que plantean riesgos^e.

Además, **varios Estados miembros de la UE han comenzado a legislar con el fin de establecer una edad mínima para acceder a los medios sociales y otros servicios digitales** que puedan exponer a niños y adolescentes a posibles daños. Por ejemplo, Francia propone en la actualidad un límite de 15 años, sobre la base de una lista negra de servicios restringidos. Grecia prevé un límite de 15 años para los servicios de redes sociales en línea. Dinamarca está estudiando un límite para los menores de 16 años, con la opción de reducir la edad con el consentimiento de los padres. Suecia plantea un límite basado en el año en que el menor cumple 15 años, con varios tipos de servicios exentos. Muchos otros, desde Portugal y España hasta Alemania y Polonia, están estudiando la posibilidad de legislar sobre este tema.

En este contexto, la fragmentación del mercado único europeo de servicios digitales constituye un riesgo real. En vista de ello, muchos Estados miembros piden que la cuestión se aborde a escala de la UE. Debe reconocerse que los Estados miembros tienen contextos culturales y nacionales diferentes en lo que respecta a la educación, la alfabetización digital y la protección de los menores. La fragmentación podría hacer que los menores disfrutasen de diferentes niveles de protección en toda la UE. Esto conllevaría además complejidades de orden práctico para las autoridades reguladoras en relación con la aplicación de las normas y unos costes derivados del cumplimiento más elevados para los proveedores. Todo ello

- a. Comisión Europea (2026). [Década digital, informe del Eurobarómetro, febrero — marzo de 2026](#).
- b. Presidencia danesa del Consejo de la Unión Europea (2026). [La Declaración de Jutlandia: Construyendo un mundo digital más seguro para los niños](#).
- c. Parlamento Europeo (2025). [Protección de los menores en línea — Resolución del Parlamento Europeo, de 26 de noviembre de 2025, sobre la protección de los menores en línea \(2025/2060\(INI\)\)](#).
- d. Consejo Europeo (2026). [Conclusiones del Consejo Europeo, 19 de marzo de 2026](#).
- e. G7 (2026). [Llamamiento de los dirigentes sobre un espacio digital más seguro para los menores](#).

podría tener repercusiones en el desarrollo de medios sociales y otros servicios digitales más seguros, así como en la eficacia de la legislación en materia de seguridad en línea.

La UE ya ha tomado medidas específicas para proteger a los menores. Las recientes decisiones adoptadas por la Comisión Europea solo han puesto de relieve con pruebas concretas la necesidad de abordar las amenazas a las que se enfrentan los niños y adolescentes en línea. Constituyen ejemplos claros las conclusiones preliminares contra Meta y TikTok por el supuesto incumplimiento de las estrictas normas de protección de los menores en línea exigidas en virtud del Reglamento de Servicios Digitales y por no proporcionar mecanismos de fácil acceso que permitan señalar contenidos de abuso sexual infantil. Además, las recientes decisiones históricas de los órganos jurisdiccionales estadounidenses han marcado un punto de inflexión significativo en el debate sobre la responsabilidad de las plataformas.

Breve historia de la protección de los menores en línea

Los esfuerzos por proteger a los niños y adolescentes en línea son tan antiguos como internet y tienen su origen en un momento anterior a los medios sociales, los teléfonos inteligentes y la IA. Las bases de las normas actuales para proteger a los menores en línea se establecieron en la década de 1990 y principios de la década de 2000, con leyes diseñadas para permitir que los servicios y las empresas operen e intercambien información a través de las fronteras. Aunque estas normas no se concibieron con el único fin de proteger a los niños y adolescentes en línea, establecieron muchos de los principios que siguen sustentando la legislación vigente en tres ámbitos.

En primer lugar, la regulación de los medios de comunicación y los servicios digitales en el mercado interior introdujo normas comunes para los servicios de televisión en toda Europa, incluidas salvaguardias contra los contenidos que pudieran ser perjudiciales para los menores. El primer marco armonizado para los servicios en línea o «servicios de la sociedad de la información» (en virtud de la Directiva sobre el comercio electrónico) también apoyó el desarrollo de servicios transfronterizos en línea dentro de la UE.

El segundo ámbito son las normas de protección de datos y privacidad, empezando por las normas comunes de la Directiva sobre protección de datos de 1995 para la recogida y el uso de información personal en todos los Estados miembros.

En tercer y último lugar, la protección de los consumidores. Las normas comunes de la UE abordan las prácticas comerciales engañosas y agresivas. Dichas normas reconocen que los consumidores vulnerables necesitan protección adicional, un principio importante en el entorno digital. Esto incluye los casos en que los niños y adolescentes están expuestos a prácticas comerciales que pueden afectarles de manera diferente a los adultos.

A medida que las tecnologías digitales se integraron profundamente en la vida cotidiana, la UE ha seguido actualizando estos marcos jurídicos para responder a los nuevos retos. El Reglamento General de Protección de Datos (RGPD) introdujo protecciones específicas para salvaguardar los datos personales y el consentimiento de los niños en línea. La Directiva de Servicios de Comunicación Audiovisual se amplió para abarcar nuevas formas de contenidos audiovisuales y plataformas de intercambio de vídeos. Por último, el Reglamento de Servicios Digitales estableció normas para los servicios intermediarios en línea, también con el fin específico de proteger a los menores.

Esta evolución refleja una tendencia más amplia: las tecnologías digitales ya no encajan claramente en una única categoría reglamentaria o jurídica. Los medios sociales y otros servicios digi-

tales combinan elementos de los medios de comunicación, la comunicación en general, el comercio y el tratamiento de datos, a menudo dentro de la misma plataforma. En consecuencia, para ser eficaz, la protección de los menores en línea debe abordarse desde un enfoque global y basarse en instrumentos en diversos ámbitos del Derecho de la Unión, como la regulación de las plataformas, la protección de datos, la protección de los consumidores y la regulación de los medios audiovisuales.

Con el rápido desarrollo y despliegue de la IA, se están superponiendo los riesgos para los menores en línea. Esto va acompañado de la evolución continua de los medios sociales y otros servicios digitales para captar y mantener la participación de los usuarios en la «economía de la atención» actual. La necesidad de que las autoridades reguladoras intervengan para reforzar la protección de los menores y capacitarlos para navegar por el mundo de los medios sociales+ de forma segura es mayor que nunca.

Las pruebas sobre los riesgos y oportunidades a los que se enfrentan los menores en línea

El rápido cambio tecnológico ha traído consigo oportunidades extraordinarias para que los niños intercambien puntos de vista con sus iguales, expresen su creatividad y accedan al conocimiento y al apoyo. Sin embargo, los niños no son adultos y el entorno de los medios sociales+ los expone a diversos riesgos para su salud física y mental y su desarrollo a diferentes edades. Los factores socioeconómicos e individuales, como el origen familiar y el género, así como el diseño de los medios sociales y otros servicios digitales, también pueden influir de forma decisiva.

Es fundamental disponer de pruebas sólidas sobre la relación entre los riesgos y los daños y los medios sociales y otros servicios digitales para fundamentar las medidas adecuadas para proteger y empoderar a los menores en línea. Las características, funcionalidades o formatos específicos utilizados en los medios sociales+ pueden ser perjudiciales en distinta medida, dependiendo de las circunstancias sociales y personales de un niño o adolescente. Los menores pertenecientes a grupos raciales, étnicos y religiosos minoritarios, los miembros de la comunidad LGBTIQ +, los que tienen necesidades educativas especiales o problemas de salud mental preexistentes pueden ser especialmente vulnerables a los perjuicios derivados de las actividades en línea. Por supuesto, esta vulnerabilidad se ve amplificada por los medios sociales y otros servicios digitales con contenidos o diseños perjudiciales, manipuladores o adictivos. A medida que estas características evolucionan, también deben hacerlo la investigación y la recopilación de pruebas.

Los riesgos para la salud física y mental que plantean los medios sociales y otros servicios digitales para los menores son amplios. En términos de salud física, un tiempo excesivo frente a la pantalla sustituye al juego al aire libre y al deporte y puede afectar a la salud, el estado físico y el sueño de los niños. El uso de medios sociales+ y dispositivos a una edad temprana desplaza la exploración práctica y las interacciones sociales presenciales. Esto puede afectar al desarrollo socioemocional y a la susceptibilidad a los problemas de salud mental. El uso prolongado de dispositivos también puede provocar problemas, como problemas musculoesqueléticos y fatiga ocular digital.

Los riesgos para la salud mental que plantea el uso de los medios sociales y otros servicios digitales para los niños son significativos. Los riesgos del entorno de los medios sociales+ que perjudican directamente la salud mental de los niños se entrecruzan con su potencial para exacerbar los problemas de salud mental preexistentes, como la depresión y la ansiedad. También en este caso, los factores sociales e individuales determinan la exposición de los niños y adolescentes a los riesgos.

En general, el elevado uso de los medios sociales y otros servicios digitales entre niños y adolescentes se asocia a problemas de sueño y concentración, así como a un aumento de las tasas de depresión y ansiedad. Las características de diseño adictivo amplifican estos efectos al fomentar la comprobación compulsiva, el «miedo a perderse algo» (FOMO) y una mayor comparación social. Esto puede erosionar la autoestima de los menores y aumentar su estrés. Los sistemas de amplificación algorítmica y de recomendación tienen el potencial de mejorar la desinformación y la incitación al odio. Estos efectos causan graves daños, en particular, a los grupos vulnerables en línea.

Los riesgos de exposición de los menores a contenidos delictivos e ilícitos en línea son considerables. Tanto los adultos como los menores explotan deliberadamente los medios sociales y otros servicios digitales, incluidas las plataformas de juegos, para interactuar con niños y adolescentes. Los riesgos incluyen la exposición al abuso sexual de menores (material), la captación de menores, el ciberacoso, la radicalización y la incitación a cometer actos ilegales, violentos o terroristas. El uso generalizado de herramientas de IA plantea graves amenazas para los niños y adolescentes derivadas de la producción de contenidos falsos de abuso sexual de menores (por ejemplo, las ultrafalsificaciones). Estos usos indebidos tienen efectos drásticos en el desarrollo de los menores, su salud mental y física y, en los casos más graves, pueden costarles la vida.

Los proveedores de medios sociales y otros servicios digitales siguen siendo los principales responsables de mantener la seguridad de los menores cuando utilicen sus servicios. Además, los padres y cuidadores desempeñan un papel importante a la hora de supervisar el tiempo en línea de los niños y adolescentes y de orientar a los menores a la hora de abordar juntos los riesgos a los que se enfrentan en los entornos de los medios sociales+. Garantizar actividades no digitales e interacciones en persona adecuadas es crucial a todas las edades.

A pesar de los múltiples daños potenciales, **el mundo de los medios sociales+ ofrece muchas oportunidades a los niños y adolescentes.** Cuando los menores están capacitados para interactuar de forma segura en línea y tienen capacidades digitales sólidas, el uso de los medios sociales y otros servicios digitales puede favorecer el bienestar, la conexión social, proporcionar redes de apoyo entre iguales, oportunidades para la autoexpresión, el compromiso cívico y el aprendizaje independiente. Las iniciativas específicas en materia de capacidades digitales — como la estrategia «Una Internet mejor para los niños» de la UE, los Centro de Seguridad en Internet y la integración de la alfabetización mediática en los planes de estudio nacionales de educación y formación— han demostrado su capacidad para mejorar el pensamiento crítico, la resiliencia frente a la desinformación y la capacidad de los menores para desenvolverse de forma segura en línea.

Las redes sociales y otros servicios digitales «seguros desde el diseño» podrían contribuir al empoderamiento y la participación en línea de niños y adolescentes apoyando la adquisición de capacidades digitales y la alfabetización mediática. La educación digital adaptada a la edad impartida por los centros educativos con el apoyo de padres y cuidadores también podría equipar a los menores para aprovechar las oportunidades del mundo digital y gestionar los posibles riesgos y daños.

La necesidad de abordar los riesgos específicos de cada edad

A medida que los niños crecen y se hacen más independientes, disminuye la capacidad de los padres para supervisar sus actividades en internet y aumenta el papel de la influencia de los compañeros. Duran-

te la adolescencia, a medida que llegan a la mayoría de edad, los menores son cada vez más autónomos en el uso de internet y más capaces de comprender y abordar los riesgos a los que están expuestos en internet. Naturalmente, a los 3 años no se tienen las mismas necesidades que a los 16, lo que pone de relieve la **importancia de que el enfoque en materia de seguridad infantil en internet sea sensible a la fase del desarrollo**, como el que se aplica en el presente informe, **diferenciando entre distintos grupos de edad**:

Los menores de 3 años sufren principalmente riesgos relacionales y «tecnointerferencias»^f como usuarios pasivos en internet. Los riesgos se derivan en gran medida del hecho de que los cuidadores sustituyen la interacción directa por pantallas para «calmar» o distraer a los niños pequeños. Esto puede afectar a la capacidad de atención de los niños, la adquisición del lenguaje y el desarrollo socioemocional.

Entre los 3 y los 5 años, los niños se inician como usuarios independientes con supervisión y son cada vez más vulnerables a los riesgos presentes en los entornos en línea derivados de una mayor exposición a las pantallas. Los medios sociales y otros servicios digitales que están optimizados para generar gratificación inmediata, recompensas repetitivas y continua estimulación externa no se ajustan en absoluto a las capacidades aún en desarrollo de los niños y pueden perjudicar su desarrollo a largo plazo.

Entre los 6 y los 9 años, el uso de los medios sociales y otros servicios digitales por parte de los niños se expande significativamente. La validación externa procedente del entorno digital (como los «likes», las puntuaciones o las clasificaciones) interfieren con una autoestima incipiente, sustentada en las competencias que los niños van adquiriendo en el mundo real. Esto les puede agravar la ansiedad al comparar su rendimiento con los compañeros, aumentando así su vulnerabilidad al ciberacoso, la incitación al odio y el acoso por parte de compañeros.

Entre los 10 y los 12 años, el acceso de los niños a los espacios de los medios sociales+ se convierte en un requisito previo esencial para la participación social. A esta edad, los niños se encuentran en una etapa en la que convergen del modo más crítico las vulnerabilidades de su desarrollo y la amplificación generada por las plataformas. Los sistemas de recomendación algorítmica intensifican la comparación social, la exposición a contenidos nocivos o ilícitos (como el abuso sexual de menores, la propaganda extremista y la desinformación) y a patrones de diseño adictivos que aumentan los síntomas de la depresión y la ansiedad. Estudios prospectivos recientes sugieren que la adquisición de un teléfono inteligente por primera vez a los 12 años (en lugar de a los 13) puede estar relacionada con un mayor riesgo de depresión y otros problemas de salud mental al cabo de un año^g. Este ejemplo pone de relieve que, en general, los niños menores de 13 años son especialmente vulnerables.

Entre los 13 y 15 los años, los adolescentes pasan del uso de los medios sociales y otros servicios digitales bajo supervisión al uso autónomo progresivo. A esta edad, las formas tradicionales de supervisión por parte de cuidadores y educadores escolares resultan cada vez más ineficaces. Los riesgos proceden cada vez más de las estructuras de los medios sociales y otros servicios digitales, más que del comportamiento individual por sí solo. Un reto clave reside en abordar los sistemas algorítmicos que estructuran la exposición e influyen en el comportamiento y funcionan con una transparencia limitada.

^f. La interrupción de la interacción entre padres e hijos por la tecnología.

^g. Hospital Infantil de Filadelfia (2026). [Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study](#). (Los límites de edad por sí solos no evitan los riesgos de los teléfonos inteligentes, sugiere el estudio del Hospital Infantil de Filadelfia). Consultado el 12 de julio de 2026.

La transición a la autonomía es una parte normal del crecimiento en el mundo actual de internet, al igual que en el mundo real. Por lo tanto, la cuestión no es cómo frenar la transición de los adolescentes a la autonomía, sino cómo limitar su exposición a peligros durante una fase de su desarrollo en la que la vulnerabilidad es máxima. Una protección eficaz requiere un enfoque multinivel diferenciado por fases del desarrollo que combine la regulación de los medios sociales y otros servicios digitales, las intervenciones educativas y el apoyo a la autorregulación y al uso crítico de los medios de comunicación.

Por último, **entre los 16 y los 18 años**, los adolescentes se encuentran en una fase en la que se desarrollan tanto la consolidación de la identidad como la autonomía. La evolución de las capacidades de los adolescentes les capacita mejor para comprender y gestionar los riesgos a los que se enfrentan en internet. Sin embargo, el desarrollo neurobiológico dista mucho de haberse completado y los riesgos de adicción, ansiedad y problemas de salud mental se ven exacerbados por el uso de los medios sociales y otros servicios digitales. Los adolescentes a esta edad deben adquirir las capacidades necesarias (por ejemplo, de pensamiento crítico y de evaluación) para navegar con éxito y seguridad por el mundo digital y aprovechar todo su potencial.

Seis principios rectores para proteger y empoderar a los menores en internet

La presencia tanto de riesgos como de oportunidades para los niños y adolescentes en el entorno de los medios sociales+ requiere un marco político global que proteja y empodere a los menores en internet. Los siguientes **Seis Principios Rectores elaborados por los copresidentes orientaron el trabajo del Grupo Especial** y se reflejan en la estructura del presente informe. Las medidas deben basarse en pruebas y análisis sólidos de los retos y oportunidades a los que se enfrentan los niños en internet. La aplicación y evaluación efectivas son fundamentales para lograr los resultados.

PRINCIPIO 1

Enfoque por fases del desarrollo (véase el capítulo 1)

Garantizar unas normas adecuadas a cada edad y orientaciones diferenciadas por edades. El desarrollo por etapas de niños y adolescentes exige el diseño y el despliegue de medidas de protección que aborden los riesgos a los que se enfrentan a edades específicas. Cuando sea posible, estas medidas deberían tener en cuenta las circunstancias personales y sociales de los niños, las cuales pueden agravar su exposición al riesgo.

PRINCIPIO 2

Igualdad y diversidad (véase el capítulo 2)

Reconocer que edades y grupos socioeconómicos diferentes implican una desigualdad en los riesgos y la exposición a los peligros de internet. El género, la sexualidad, el origen racial, étnico y religioso, las necesidades educativas especiales y los problemas de salud mental preexistentes determinan la vulnerabilidad de los menores a los peligros de internet. Estos factores también influyen en los recursos y capacidades que los padres y cuidadores tienen para apoyar a los niños y adolescentes en su camino hacia la autonomía.

PRINCIPIO 3**Protección de los menores (véase el capítulo 3)**

Los niños y adolescentes deben poder utilizar espacios seguros en los medios sociales+. En el diseño de los medios sociales y otros servicios digitales debería incorporarse la protección de los menores contra los contenidos nocivos, las características adictivas, la negligencia digital ^{viii} y los delitos en línea (por ejemplo, el abuso sexual). Debería ser fácil que los menores puedan denunciar cualquier contenido o elemento nocivo. Debería darse prioridad a estas denuncias y los proveedores deberían retirar rápidamente los contenidos o elementos nocivos.

PRINCIPIO 4**Responsabilidad de los servicios digitales y derechos de los consumidores (véase el capítulo 3)**

Los proveedores de medios sociales y otros servicios digitales deben asumir la responsabilidad primaria de garantizar que los espacios en línea sean seguros para que los menores accedan a ellos y los utilicen. Incentivar la adopción de medidas de seguridad en los servicios digitales ya en la fase del diseño y aplicar rápidamente una regulación sobre los contenidos. La carga de la prueba de que las características de sus servicios no son perjudiciales debe recaer sobre los proveedores de medios sociales y otros servicios digitales, antes de que puedan acceder a niños y adolescentes.

PRINCIPIO 5**Empoderamiento y educación en medios de comunicación (véase el capítulo 4)**

Capacitar a padres y cuidadores, profesores y educadores para apoyar la transición gradual de los niños y adolescentes hacia un uso de internet seguro y autónomo. Ofrecer suficientes oportunidades (por ejemplo, formación en alfabetización digital y mediática) y una infraestructura adecuada para que los padres puedan reflexionar sobre sus propias actividades y orientar las interacciones en internet de los menores. Las medidas deben adaptarse a las funciones de los cuidadores y educadores, que evolucionan a medida que los niños y adolescentes maduran.

PRINCIPIO 6**Derechos y participación de los niños (véase el capítulo 4)**

Salvaguardar el derecho de los niños a la participación, la interacción y la creación conjunta seguras, tanto en internet como en el mundo real. Los derechos del niño, tal como se entienden en los marcos

h. La omisión reiterada por parte de un cuidador de sus deberes de atención, capacidad de respuesta, supervisión o protección adecuadas del desarrollo de un menor debido a que las tecnologías digitales interfieren con las funciones asistenciales esenciales, las sustituyen o las disminuyen.

internacionales pertinentes,ⁱ deben sustentarse siempre las medidas de protección de la infancia. Las restricciones de edad deben respetar los derechos del niño en internet, ser proporcionadas, limitadas en el tiempo y equilibradas con el interés superior del niño. Esto también pone de relieve la necesidad de invertir en actividades al margen de internet para menores de todas las edades y de promoverlas.

Consejeros especiales del presidente y copresidentes del Grupo Especial sobre Seguridad Infantil en Línea



Prof. Dr. Jörg M. Fegert
*Director médico del Departamento
 de Psiquiatría Infantil y Juvenil,
 Psicosomática y Psicoterapia del
 Hospital Universitario de Ulm.*



Dra. Maria Melchior
*Directora de investigación del
 Instituto Nacional de Salud
 e Investigación Médica de
 Francia (INSERM)*

- i. En particular, la Convención de las Naciones Unidas sobre los Derechos del Niño y las Observaciones generales del Comité de los Derechos del Niño, la Carta de los Derechos Fundamentales de la Unión Europea y la Estrategia de la UE sobre los Derechos del Niño.

SEIS PRINCIPIOS RECTORES

Para proteger y empoderar a los menores en internet

S E G U R I D A D I N F A N T I L E N I N T E R N E T

ANÁLISIS DE LA SITUACIÓN

ENFOQUE POR FASES DEL DESARROLLO

Asegurar una regulación adecuada a la edad y orientaciones diferenciadas

IGUALDAD Y DIVERSIDAD

Reconocer que los diferentes grupos están expuestos a riesgos y peligros digitales distintos

PROTECCIÓN DE LOS MENORES

Proteger contra los contenidos nocivos, el diseño adictivo, el abandono digital y los delitos (p.ej., abuso sexual, acoso)

RESPONSABILIDAD DE LOS SERVICIOS DIGITALES Y DERECHOS DE LOS CONSUMIDORES

Incorporar la seguridad y la regulación del contenido desde el diseño

EMPODERAMIENTO Y EDUCACIÓN EN MEDIOS DE COMUNICACIÓN

Posibilitar que padres y cuidadores ayuden a los menores a usar responsablemente las habilidades digitales y la alfabetización mediática

DERECHOS Y PARTICIPACIÓN DE LOS NIÑOS

Salvaguardar el derecho a la participación y la cocreación en internet con seguridad

MEDIDAS

EVALUACIÓN

Recomendaciones clave para proteger y empoderar a los menores en internet

El objetivo general de las recomendaciones del presente informe, basado en un enfoque sensible a las fases del desarrollo y que refleja los seis principios rectores, es equilibrar la necesidad de proteger a niños y adolescentes en internet con su derecho a participar y aprovechar las oportunidades del mundo de los medios sociales.

Recomendaciones sobre el uso adecuado a la edad de los medios sociales y otros servicios digitales

DE 0 A 2 AÑOS

Evitar las pantallas y los medios sociales+

Evitar en gran medida la exposición a pantallas durante la primera infancia no significa una prohibición total. De hecho, reconoce las necesidades de desarrollo de los niños en cuanto al apego, el desarrollo sensorial y la adquisición temprana del lenguaje. Los padres y cuidadores deben dar prioridad a las interacciones presenciales y ser conscientes de su propio uso de los dispositivos digitales para ofrecer un modelo positivo y evitar la «tecnointerferencia». Este enfoque está en consonancia con las recomendaciones de la Organización Mundial de la Salud para evitar alteraciones en el desarrollo neurobiológico y cognitivo de los niños y en la formación de vínculos emocionales, así como problemas físicos (por ejemplo, que afecten a la visión).

DE 3 A 12 AÑOS:

Uso supervisado de medios sociales+ y dispositivos adecuados a la edad

No debe permitirse a los niños el uso no supervisado de dispositivos con acceso a internet. Los centros educativos deben acondicionar instalaciones para el uso supervisado y limitado de dispositivos con fines educativos, fomentando la alfabetización digital y mediática, la resiliencia emocional y la reflexión crítica sobre los riesgos. Los padres y cuidadores deben supervisar y apoyar gradualmente la autonomía digital con medios sociales y otros servicios digitales adecuados a la edad. También deben conversar regularmente con los niños sobre los posibles beneficios y riesgos de las interacciones de los menores en internet. Tanto los cuidadores como los educadores deben seguir animando a los niños de esta edad a participar en actividades al margen de internet.

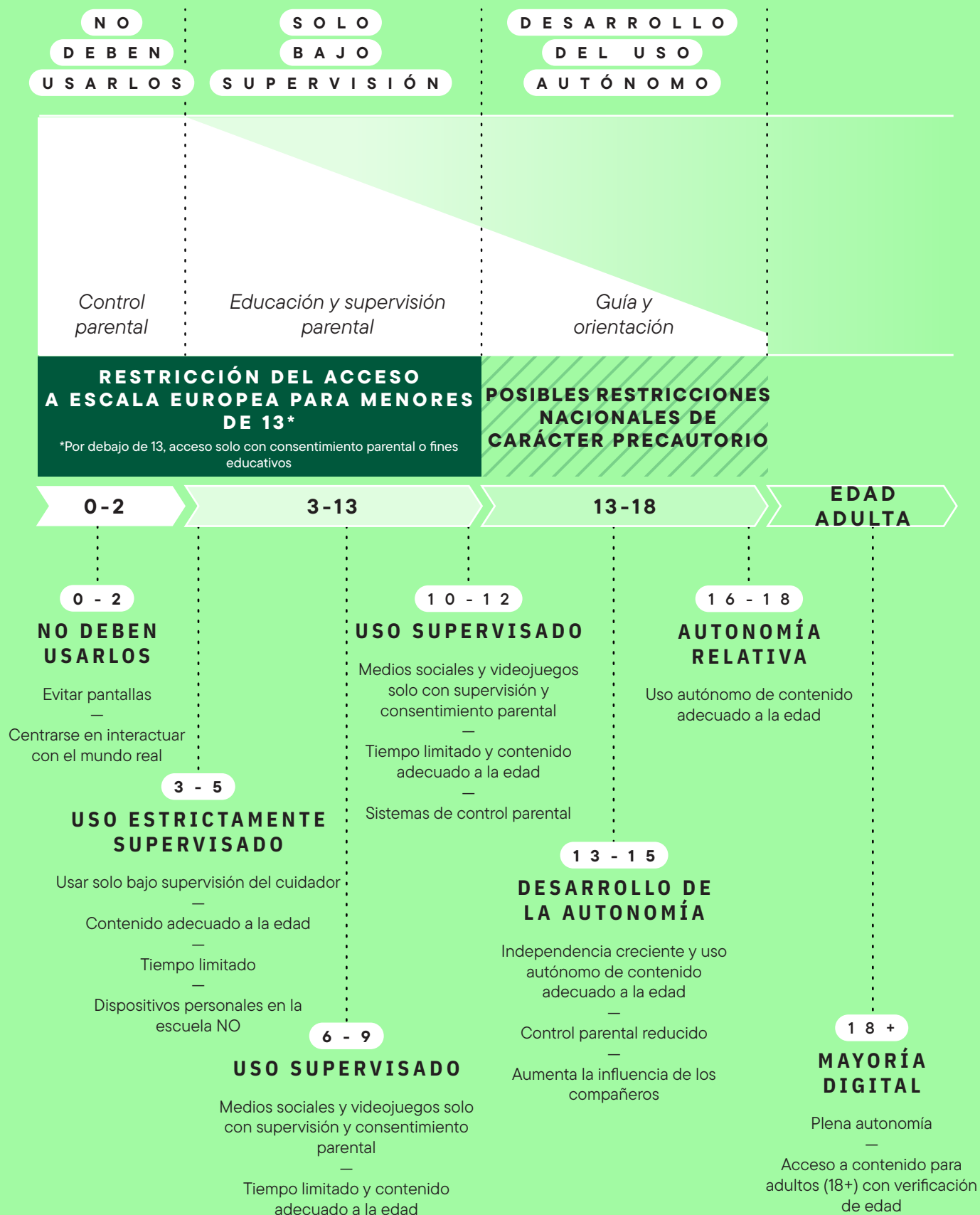
DE 13 A 18 AÑOS:

Evolución del uso autónomo de los medios sociales+ adecuados a la edad

De 13 a 18 años, los adolescentes solo deberían tener acceso a medios sociales y a otros servicios digitales adecuados a su edad y «seguros por defecto» que hayan introducido activamente funciones de seguridad clave (por ejemplo, límites al *scroll* infinito y a los sistemas de recomendación). Hasta que

se desarrollen estos medios sociales y otros servicios digitales «seguros por defecto», el control y la supervisión parental individual adecuada a la edad siguen siendo esenciales. Podría considerarse la adopción de medidas preventivas adicionales por parte de las autoridades reguladoras. A medida que los adolescentes mayores de 16 años avanzan hacia una mayor autonomía digital, persisten los riesgos relacionados con la exposición a contenidos nocivos en internet. Los padres y cuidadores deben seguir conversando con los menores sobre sus experiencias en internet. Los adolescentes deberían tener un acceso privilegiado a los servicios de ayuda y a los sistemas de reclamaciones, y al mismo tiempo beneficiarse de redes de ayuda entre compañeros que promuevan el uso responsable de los medios sociales y otros servicios digitales.

Edades adecuadas para que los menores usen los medios sociales+



Recomendaciones para proteger a los niños y adolescentes en internet

// Proponer una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años.

Una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años. Una restricción armonizada del acceso facilitaría la aplicación de mecanismos de control de la edad proporcionados y respetuosos de los derechos, e impulsaría los requisitos de seguridad desde el diseño para los proveedores de medios sociales y otros servicios digitales. Los menores de 13 años deben tener un acceso de duración limitada a entornos de medios sociales+ adecuados a su edad, únicamente con autorización y supervisión parental o en contextos educativos. A partir de los 13 años, el uso que hacen los adolescentes de los medios sociales y otros servicios digitales adecuados a su edad y seguros debe poder evolucionar hacia la autonomía.

Unas normas armonizadas a escala de la UE sobre una edad mínima de 13 años contribuirían al correcto funcionamiento del mercado único al garantizar un marco único de cumplimiento para los proveedores. Las normas armonizadas facilitarían la aplicación y la supervisión por parte de las autoridades reguladoras, tanto a escala nacional como de la UE. También garantizarían un mismo nivel de protección para todos los menores en internet en toda la UE, independientemente de los contextos socioeconómicos, culturales y nacionales.

// Introducir sistemas eficaces de control de la edad para aumentar la seguridad ya desde el diseño y enfoques adecuados a la edad para proteger y empoderar a los menores en internet.

Los métodos de control de la edad —tanto la verificación como la estimación— deben ser proporcionados y respetar unos requisitos mínimos, en particular en lo que respecta a los derechos fundamentales de los usuarios, incluidos los derechos de los menores y las garantías conexas. Cualquier método empleado para comprobar la edad debe respetar las normas más estrictas en materia de privacidad y protección de datos, y no debe implicar el tratamiento de los documentos de identidad ni de los datos biométricos con el fin de estimar la edad. Deben implantarse normas técnicas, como la «prueba de conocimiento cero», a fin de garantizar que ni la plataforma encargada de evaluar la edad ni el proveedor de verificación de la edad reciban información alguna que permita rastrear o identificar al usuario.

Los métodos de control de la edad deben determinar con precisión la edad o los grupos de edad requeridos, y ser fáciles y fiables en la práctica, en condiciones reales. Los métodos deben ser sólidos para evitar su elusión y las amenazas a la ciberseguridad, inclusivos (y no discriminatorios) y estar disponibles por igual para todas las personas que necesiten utilizarlos. Los proveedores de medios sociales y otros servicios digitales deben cumplir su obligación de evitar que los menores se vean expuestos a servicios de riesgo y que haya usuarios que se hagan pasar por niños y adolescentes.

// Ampliar y armonizar las normas sobre las características clave de seguridad en el diseño de las redes sociales y otros servicios digitales.

Los medios sociales y otros servicios digitales debería incorporar salvaguardias claras de seguridad desde el diseño y adecuadas a la edad (por ejemplo, posibles límites al *scroll* infinito, a la reproducción automática, a las notificaciones automáticas y a los motores de recomendación personalizados problemáticos).

Para hacer frente al diseño que genera adicción, los patrones oscuros, el contacto no solicitado y las espirales de contenido, los ajustes predeterminados de protección deberían ser parte integrante de los medios sociales y otros servicios digitales. La ampliación y armonización de las normas sobre los elementos clave de seguridad garantizaría la seguridad y la uniformidad en todo el entorno de las redes sociales+. Debido al rápido desarrollo de la tecnología, cualquier norma sobre características clave de seguridad debería ser adaptable para poder abordar en permanencia nuevas características nocivas de diseño.

// Trasladar la carga de la prueba de que sus productos y servicios son seguros para los menores a los medios sociales y otros proveedores de servicios digitales.

Deberían aplicarse restricciones específicas de edad hasta que los proveedores de medios sociales y otros servicios digitales introduzcan elementos clave de diseño de seguridad que protejan a los niños y adolescentes. Hasta que los proveedores no demuestren haber incorporado elementos seguros y adecuados a la edad, cumpliendo así las medidas nacionales y de la UE, no deberían tener acceso a los menores. Cuando exista una versión «segura por defecto», los elementos inadecuados para la edad (elementos para adultos) solo deberían activarse tras unos controles de la edad eficaces.

// Reforzar las capacidades de ejecución y evaluación.

Habida cuenta de las múltiples normas que se aplican actualmente a la seguridad infantil en internet (el Reglamento de Servicios Digitales, el Reglamento General de Protección de Datos, el Reglamento de Inteligencia Artificial, etc.), las autoridades de control deberían intensificar la cooperación y el intercambio de información entre los marcos jurídicos. Esto es fundamental para evitar incoherencias y garantizar un entorno jurídico coherente, predecible y eficaz basado en la protección de los derechos fundamentales. La Comisión Europea debería explorar mecanismos que permitan una cooperación fluida entre las autoridades de supervisión para aprovechar las estructuras de ejecución existentes. Además, es necesario valorar si se necesitan recursos adicionales y reestructuración para las autoridades reguladoras responsables de la aplicación y la evaluación. Deberían considerarse actuaciones para reforzar el papel de la sociedad civil en la ejecución y su contribución a la capacidad de ejecución, también a través de las estructuras existentes. La ejecución debería ser complementaria y evitar actuaciones contradictorias.

// Adoptar rápidamente medidas para garantizar que los proveedores de medios sociales y otros servicios digitales tengan obligaciones claras para prevenir, detectar, denunciar y bloquear el abuso sexual de menores en internet, también en las comunicaciones interpersonales.

Debería colmarse rápidamente la laguna en materia de seguridad infantil que existe actualmente debido a la expiración del Reglamento provisional por el que se establecen normas para prevenir y combatir el abuso sexual de menores. Los legisladores de la UE deberían adoptar rápidamente la propuesta de Reglamento para el largo plazo destinado a prevenir y combatir el abuso sexual de menores. Más del 80 % de las investigaciones de abuso sexual de menores parten de denuncias presentadas por los proveedores de medios sociales y otros servicios digitales. A menudo, los menores tienen demasiado miedo a denunciar abusos. Detectar material de abuso sexual de menores, también en las comunicaciones interpersonales, es a menudo la única manera de detenerlo.

// Los Estados miembros pueden introducir restricciones preventivas adicionales de acceso a los medios sociales y otros servicios digitales a partir de los 13 años.

Las restricciones prudenciales adicionales de acceso deben ser complementarias a la restricción de acceso a los medios sociales y otros servicios digitales a escala de la UE contemplada en el punto 13. Los adolescentes solo pueden tener acceso a un entorno de medios sociales+ que sea seguro, tanto en contenidos como en las características de diseño, adecuado a la edad y diseñado teniendo en cuenta sus derechos y necesidades. Los Estados miembros tienen diversos contextos históricos y nacionales diversos y pueden preferir fijar un umbral de edad superior a los 13 años. Todas las restricciones nacionales de acceso prudenciales adicionales deberían estar sujetas a una evaluación continua y, en su caso, reevaluarse, una vez que los medios sociales y otros servicios digitales sean seguros por defecto para niños y adolescentes.

// Reforzar la aplicación de las normas sobre el acceso de los investigadores a los datos y su control.

El acto delegado de julio de 2025 relativo al artículo 40 del Reglamento Delegado de Servicios Digitales ha abierto, en principio, una nueva vía para que los investigadores autorizados accedan a los datos de las plataformas en línea. Estos datos pueden utilizarse para llevar a cabo investigaciones que contribuyan a la detección, identificación y comprensión de los riesgos sistémicos, así como a la evaluación de las medidas de mitigación de riesgos que promueven la seguridad infantil en internet.

Que esta vía cumpla su cometido depende del cumplimiento por parte de los proveedores de medios sociales y otros servicios digitales y de la aplicación efectiva por parte de las autoridades reguladoras. También se basa en la extensión de los servicios cubiertos y en la calidad y continuidad de los datos facilitados. La Comisión debería evaluar el funcionamiento operativo de los requisitos del acceso a datos y el escrutinio del artículo 40 tras la experiencia inicial de los investigadores al amparo del acto delegado. Esto es fundamental para garantizar que las plataformas en línea hagan un seguimiento de las solicitudes de acceso a los datos con fines de cumplimiento, evaluación de riesgos e investigación.

Las obligaciones de acceso a los datos no solo son un elemento clave del conjunto de instrumentos de transparencia del Reglamento de Servicios Digitales, sino que también forman parte de las responsabilidades más amplias de mitigación de riesgos de los proveedores de medios sociales y otros servicios digitales. También debe alentarse a las plataformas más pequeñas a que permitan a los investigadores acceder a los datos, teniendo en cuenta los riesgos que estas plataformas plantean para los menores y el papel del escrutinio independiente a la hora de abordar estos riesgos. El uso de los principios rectores FAIRⁱ para la gestión y administración de datos científicos debe ser la norma en la aplicación del artículo 40.

ⁱ. Los principios rectores FAIR para la gestión y administración de datos científicos se introdujeron en 2016 en una publicación de la revista *Scientific Data*. Los principios tienen por objeto mejorar la infraestructura de apoyo a la reutilización de datos académicos mediante el refuerzo de la capacidad de las máquinas y de las personas para encontrar y utilizar datos. Véase: Wilkinson, M.D., et al. (2016). [The FAIR Guiding Principles for scientific data management and stewardship](#) (Los principios rectores FAIR para la gestión y administración de datos científicos). Datos científicos, 3.

Recomendaciones para empoderar a los niños y adolescentes en línea

// Ampliar las oportunidades seguras para que los menores participen activamente en la configuración del entorno de los medios sociales y otros servicios digitales.

Los niños y adolescentes deben tener oportunidades significativas para configurar activamente la legislación, las políticas y las iniciativas educativas que promuevan la seguridad y el empoderamiento de los niños en línea. Debe ampliarse el uso de las herramientas de participación infantil y juvenil para fundamentar este trabajo. Más concretamente, debe incluirse a los niños en el diseño conjunto de las políticas de seguridad, los programas de formación, las evaluaciones y las directrices. Las medidas deben ser objeto de un seguimiento y una evaluación continuos para valorar su impacto en la seguridad y los derechos de los niños.

Los procesos de participación deben garantizar que los niños reciban información clara, comprendan cómo se utilizarán sus contribuciones y reciban comentarios sobre los resultados. Deben realizarse esfuerzos especiales para incluir a los niños de grupos desfavorecidos, marginados y vulnerables. Todas las actividades de participación que impliquen a niños deben ir acompañadas de medidas de salvaguardia adecuadas.

// Reforzar los mecanismos de denuncia y los derechos de los consumidores para niños y adolescentes.

Los proveedores de medios sociales y otros servicios digitales deben dar prioridad a los informes y quejas de niños y adolescentes en los procedimientos de moderación de contenidos. Deben reforzarse las obligaciones de los proveedores en virtud de los marcos existentes para financiar adecuadamente las líneas telefónicas de ayuda y los mecanismos de reclamación. Estos mecanismos deben ser adecuados para la edad, fáciles de usar, accesibles, respetuosos de la privacidad y eficaces.

// Integrar acciones de educación y alfabetización digitales para menores, padres y cuidadores, profesores y educadores.

La educación y la alfabetización digitales deben integrarse en todos los niveles educativos como una competencia básica clave para los menores, los padres y los profesores. El bienestar digital debe integrarse en la educación digital para todos.

La educación debe permitir a los niños y adolescentes evaluar de forma crítica la información y las fuentes en línea y reconocer las técnicas de manipulación, como la desinformación, las falsedades profundas y la publicidad personalizada. También debe lograr que los menores, los padres y los profesores comprendan cómo se crean y comparten los contenidos digitales y cómo los algoritmos configuran lo que los usuarios ven y experimentan en el mundo de los medios sociales y otros servicios digitales.

La educación estructurada en materia de seguridad en línea debe desarrollar capacidades prácticas para proteger los datos personales, gestionar los ajustes de privacidad, mantener identidades digitales seguras e identificar los riesgos en los medios sociales, los mensajes y los entornos de juego en particular. Estas capacidades deben desarrollarse progresivamente, empezando por los hábitos básicos de seguridad y avanzando hacia una comprensión más compleja de las huellas digitales, el consentimiento

y los riesgos de las plataformas. El uso saludable de pantallas debe abordarse mediante orientaciones sobre el equilibrio, la gestión de la atención y el reconocimiento de patrones de uso excesivos o nocivos.

// Crear más oportunidades e infraestructuras adecuadas para apoyar las actividades fuera de línea.

Los Estados miembros y las autoridades locales deben mantener y ampliar el acceso a deportes, artes, clubes juveniles, bibliotecas y espacios comunitarios asequibles para fomentar una participación saludable en el mundo real y crear alternativas atractivas al uso excesivo de pantallas entre los menores. Esto debe incluir la inversión en entornos seguros, inclusivos y adaptados a la edad en los que los menores puedan conectar, aprender, jugar y establecer relaciones positivas dentro de sus comunidades.

// Promover la creación conjunta de directrices para los padres.

Junto con las asociaciones de padres, la UE y los Estados miembros deben promover el desarrollo de directrices para padres. Las directrices podrían proporcionar asesoramiento claro y accesible para capacitar a los padres y cuidadores a la hora de apoyar el uso seguro, responsable y positivo de los menores con los entornos de los medios sociales y otros servicios digitales. Las directrices deben proporcionar asesoramiento práctico sobre ámbitos clave, como la seguridad y la privacidad en línea, el bienestar digital, el uso ético y responsable y el acceso al apoyo.

// Garantizar una financiación pública suficiente y normas comunes para las organizaciones de la sociedad civil y el asesoramiento entre iguales.

La UE y los Estados miembros deben velar por que los Centros de Seguridad en internet y organizaciones comparables de la sociedad civil sigan recibiendo recursos financieros suficientes y su trabajo se base en normas comunes elaboradas por expertos. Esto es vital para mantener y seguir desarrollando sus actividades, incluidos los servicios de sensibilización, formación y apoyo. La financiación pública es crucial para garantizar la independencia y la cohesión.

La financiación también debe apoyar un mayor desarrollo del asesoramiento entre iguales, las líneas de ayuda, las líneas directas, los recursos educativos, las campañas de sensibilización y las actividades de desarrollo de capacidades. Deben destinarse inversiones adicionales para aumentar la visibilidad, la accesibilidad y el alcance de estos instrumentos, también entre los menores vulnerables, y para apoyar iniciativas que promuevan entornos más seguros en los medios sociales y otros servicios digitales.

// Poner a disposición financiación a largo plazo para la investigación longitudinal europea a gran escala y seguir apoyando los ensayos aleatorios de control.

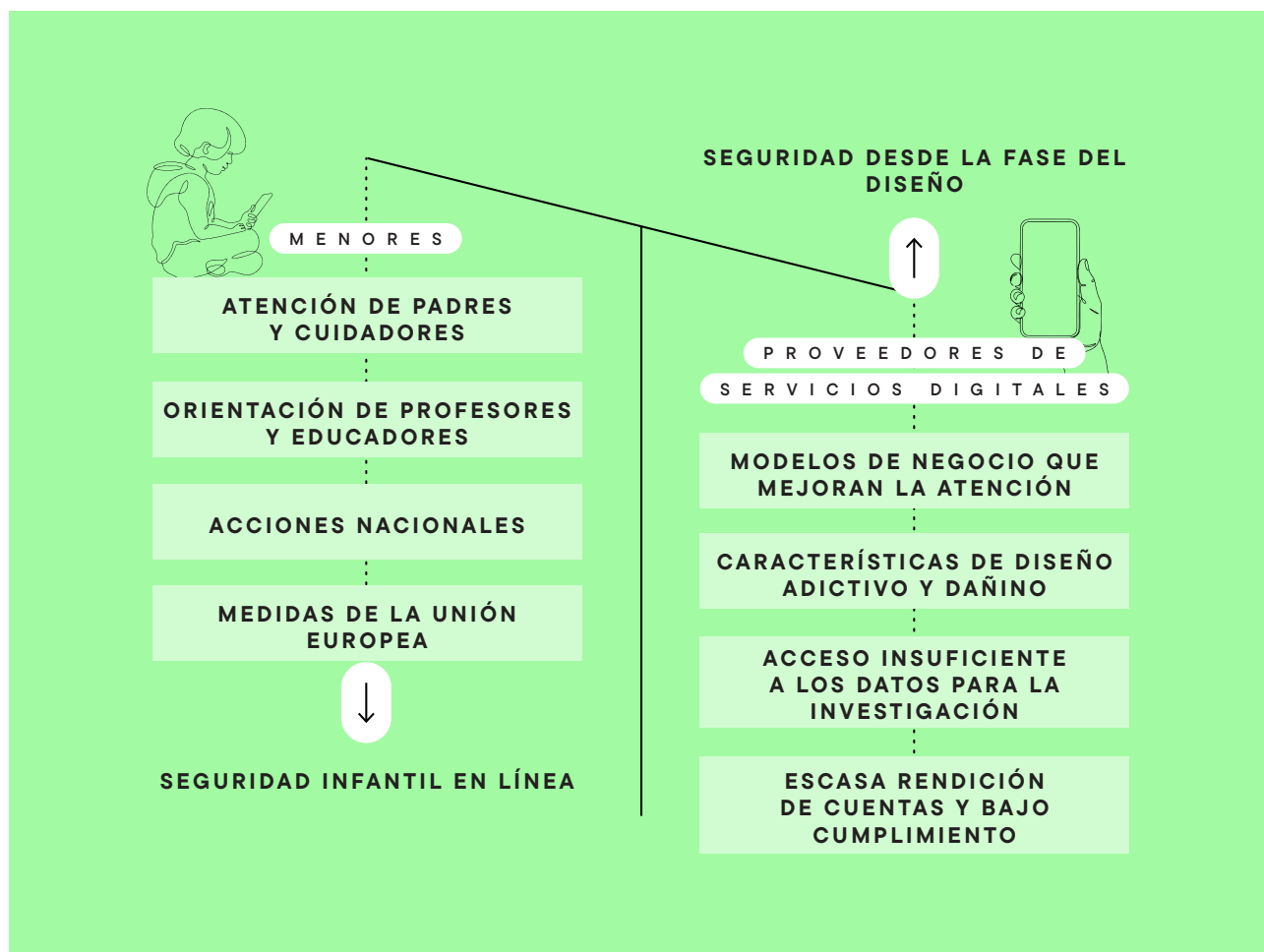
Ejemplos como el North American Adolescent Brain Cognitive Development (ABCD) Study [«Estudio sobre el desarrollo cognitivo cerebral en adolescentes de América del Norte» (ABCD, por sus siglas en inglés)]^k podrían inspirar la investigación longitudinal europea a gran escala relacionada con la seguridad

k. El estudio ABCD antes citado es el mayor estudio a largo plazo sobre el desarrollo cerebral y la salud infantil en los Estados Unidos. El estudio sigue la evolución del comportamiento de más de 11 000 niños de entre 9 y 10 años a través de la adolescencia hasta la edad adulta. Los datos recopilados permitirán la creación de normas de referencia para el desarrollo cerebral de los adolescentes y examinarán las influencias del sexo, el género, el sueño, la actividad física y el tiempo de visualización en el desarrollo de los adolescentes. Sus conclusiones también ayudarán a comprender el desarrollo de los problemas de salud mental durante la adolescencia y su relación con el abuso de sustancias.

infantil en línea. La disponibilidad de pruebas longitudinales europeas a gran escala (que abarquen un período de diez años o más) es importante para apoyar un enfoque neurobiológico y de desarrollo de la seguridad infantil en línea. Esto ayudaría a abordar las lagunas en las conclusiones en gran medida correlativas en el contexto europeo relacionadas con el impacto del uso de las redes sociales y otros servicios digitales en el desarrollo de los menores adolescentes, su salud física y mental y su exposición a daños por su actividad en línea.

Los ensayos aleatorios de control también son fundamentales para reforzar la base empírica de las políticas. La financiación de la investigación debe apoyar explícitamente los enfoques de desarrollo y psicopatología que investigan la susceptibilidad de los menores a los riesgos en línea, influidos por factores sociales e individuales en la infancia y la adolescencia.

Gráfico 2: Equilibrar el ecosistema: seguridad desde la fase del diseño en los entornos de los medios sociales y otros servicios digitales



Seguridad en línea

CONSEJOS PARA NIÑOS Y ADOLESCENTES



Conoce tus derechos: recuerda que tienes derecho a estar seguro y a ser respetado en línea.



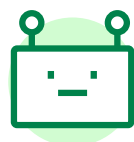
Se amable con los demás en línea: las redes sociales y los juegos deben ser una experiencia positiva para todos. Trata a otras personas con el respeto con el que le gustaría que te trataran a ti.



Piensa antes de publicar: las fotos, los vídeos y los comentarios pueden permanecer en línea para siempre. Comparte ahora solo lo que no te disgustaría que otros pudieran ver años después.



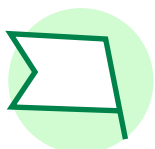
Protege tus datos personales: no compartas en línea datos privados tales como tu nombre completo, dirección, centro escolar, número de teléfono, contraseñas o localización en directo.



Recuerda que la IA es una herramienta, no una persona real: la IA puede cometer errores y crear información falsa, imágenes falsas, vídeos, voces y mensajes.



Comprueba antes de confiar o compartir: no todo en línea es cierto. Cuestiona siempre la información, especialmente las historias, vídeos o mensajes sorprendentes, y comprueba las fuentes fiables antes de compartirlas.



Reconoce el peligro: detente y piensa en peticiones extrañas de «amigos de amigos», ofertas «demasiado buenas para ser verdaderas» o mensajes que intentan presionarte para que tomes una decisión.



No aceptes fotos o peticiones de chat de extraños: si dudas de la edad o identidad de alguien, pide a un adulto que compruebe quién es (o diles que «tu padre/madre está cerca de ti» y fíjate en su reacción).



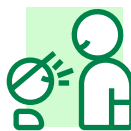
Utiliza parámetros de privacidad y seguridad: mantén tus cuentas privadas, utiliza contraseñas seguras y utiliza elementos de seguridad adicionales siempre que sea posible.



No compartas imágenes privadas: nunca compartas fotos o vídeos íntimos, aunque alguien te presione (especialmente si eres menor de 18 años). Una vez compartidas, quedan fuera de tu control.



Bloquea, denuncia y guarda pruebas: si alguien en línea te está acosando, estafando, amenazando o haciendo que te sientas incómodo, denuncia y bloquea y conserva las capturas de pantalla o mensajes.



Comparte con un adulto en el que confías los casos en que sientes que algo está mal: no estás haciendo una tontería y no te va a provocar ningún problema pedir ayuda.



Ayuda a hacer de internet un lugar más seguro: aprende cómo funcionan las aplicaciones, los juegos, los sitios web, los algoritmos y la IA, y ayuda a otros a mantenerse seguros.



Utiliza tu voz: participa y configura el futuro del mundo digital.



Seguridad en línea

CONSEJOS PARA PADRES Y CUIDADORES



Ayude a su hijo a crear hábitos de pantalla saludables: limite el tiempo de uso de la pantalla, desde la ausencia total de pantalla para niños de entre 0 y 2 años hasta límites de tiempo adecuados a la edad para niños de hasta 10 a 12 años, bajo su supervisión. En el caso de los adolescentes de 13 a 18 años, deben seguir debatiéndose los límites del tiempo de uso de pantallas, de modo que dispongan de tiempo suficiente para estudiar y reunirse con amigos de forma real.



Compruebe que las aplicaciones y los juegos están adaptados a la edad del menor.



En el caso de los niños más pequeños (hasta 12 años), **las consolas y los dispositivos solo deben utilizarse en presencia de un adulto.**



No permita los dispositivos en el cuarto de baño, en el dormitorio o a la hora de comer



Preste atención al tono de sus conversaciones en línea y durante los juegos. Busque señales de alerta.



Pasen tiempo juntos en línea: pida a su hijo que vea con usted su contenido favorito.



No critique «sus cosas»: ayude a su hijo a desarrollar su propio juicio (también obtendrá una idea de lo que sugiere su algoritmo).



Anime a su hijo a hablar con usted si le preocupa algo en línea; convénzale de que su intención es ayudarlo, no culparlo, castigarlo o arrebatarse el dispositivo.



Continúe las conversaciones sobre la seguridad en línea a medida que su hijo crece, incluso cuando tiene entre 16 y 18 años y más años.



Evite la sobreexposición de los hijos: piense cuidadosamente antes de compartir fotos o vídeos de sus hijos o adolescentes en línea. Los extraños y la IA pueden utilizar esa información de muchas maneras.



Sea un ejemplo: no esté pegado a su dispositivo cuando sus hijos estén a su alrededor. Présteles la atención que merecen y no pierda momentos y conversaciones importantes con su hijo.



Lista de todas las recomendaciones de los copresidentes por capítulo

CAPÍTULO 1:

Un enfoque de desarrollo de la seguridad infantil en línea

- // Diseñar y desplegar medidas en línea de protección de la infancia adaptadas a la edad
- // Garantizar espacios en línea seguros para los menores
- // Empoderar a los menores y sus círculos de apoyo
- // (De 0 a 2 años) — Aumentar la concienciación de los cuidadores sobre la importancia para el desarrollo de la interacción directa y humana, desde la primera infancia
- // (De 0 a 2 años) — Evitar el uso de las redes sociales y otros servicios digitales y garantizar una exposición mínima a las pantallas, en particular para los menores de 3 años
- // (De 0 a 2 años) — Limitar la difusión de datos de niños a través de perfiles de redes sociales
- // (De 3 a 12 años) — Garantizar un uso estructurado y supervisado para niños en línea
- // (De 3 a 12 años) — Ofrecer a los niños y a sus círculos de apoyo una educación digital y de bienestar de calidad
- // (De 13 a 18 años) — Garantizar la evolución del uso autónomo de los adolescentes en línea

CAPÍTULO 2:

Pruebas sobre los riesgos a los que se enfrentan los menores en línea

- // Basarse en pruebas en ámbitos poco estudiados para reforzar la elaboración de políticas basadas en datos contrastados
- // Los medios sociales y otros servicios digitales deben implicar activamente a expertos académicos independientes en el diseño de estrategias y herramientas de mitigación de riesgos
- // Se han de poner a disposición financiación a largo plazo para la investigación longitudinal europea a gran escala y seguir apoyando los ensayos aleatorios de control
- // Invertir en infraestructuras de investigación europeas seguras y compartidas para permitir un acceso seguro a los datos de los menores
- // Reforzar la aplicación de las normas sobre el acceso de los investigadores a los datos y su control

CAPÍTULO 3:

Protección de los menores en un entorno de medios sociales y otros servicios digitales en rápida evolución

- // Proponer una restricción armonizada del acceso a los medios sociales y otros servicios digitales a escala de la UE para los menores de 13 años

- // Introducir sistemas eficaces de garantía de la edad para comprobar la edad y respaldar la seguridad desde el diseño y enfoques adecuados a la edad para proteger y empoderar a los menores en línea
- // Ampliar y armonizar las normas sobre las características clave de seguridad en el diseño de las redes sociales y otros servicios digitales
- // Trasladar la carga de la prueba a los proveedores de medios sociales y otros servicios digitales para demostrar que sus productos y servicios son seguros para los menores
- // Reforzar las capacidades de ejecución y evaluación
- // Adoptar rápidamente medidas para garantizar que los proveedores de medios sociales y otros de servicios digitales tengan obligaciones claras para prevenir, detectar, denunciar y bloquear el abuso sexual de menores en línea, también en las comunicaciones interpersonales
- // Los Estados miembros pueden introducir restricciones preventivas adicionales de acceso a las redes sociales y otros servicios digitales a partir de los 13 años
- // Reforzar las políticas de protección de los consumidores para proteger a los menores en línea
- // Supervisar y evaluar continuamente el impacto de las medidas que se están aplicando
- // Al tratar los datos de los menores en virtud del RGPD, las redes sociales y otros servicios digitales deben garantizar que el interés superior del menor sea una consideración primordial
- // Garantizar la aplicación efectiva de la Directiva sobre responsabilidad por los daños causados por productos defectuosos

CAPÍTULO 4:

Capacitar a los menores para navegar con seguridad por el mundo digital

- // Ampliar las oportunidades seguras para que los menores participen activamente en la configuración del entorno de los medios sociales y otros servicios digitales
- // Reforzar los mecanismos de denuncia y los derechos de los consumidores para niños y adolescentes
- // Financiar y promover la creación y el uso de redes sociales y otros servicios digitales basados en valores de la UE en los que los menores puedan interactuar de forma segura entre sí
- // Integrar acciones de educación y alfabetización digitales para menores, padres y cuidadores, profesores y educadores
- // Crear más oportunidades e infraestructuras adecuadas para apoyar las actividades fuera de línea
- // Promover la creación conjunta de directrices para los padres
- // Garantizar que los padres y los cuidadores cuenten con el apoyo continuo de herramientas de control y supervisión de última generación y actualizadas
- // Garantizar una financiación pública suficiente y normas comunes para las organizaciones de la sociedad civil y el asesoramiento entre iguales
- // Permitir que el sistema sanitario diagnostique y trate las adicciones y otros trastornos de salud mental relacionados con el uso de las redes sociales y otros servicios digitales
- // Apoyar la formación del profesorado para incluir la alfabetización digital y mediática e implicar a los padres

- // Promover la alfabetización en materia de IA como parte integrante de la educación digital
- // Las escuelas deben ofrecer oportunidades estructuradas para mejorar la salud mental y el bienestar digital
- // Las respuestas educativas deben prestar especial atención a los grupos vulnerables
- // Invertir en infraestructuras digitales educativas seguras, preventivas, sólidas y fiables

01

Un enfoque de la seguridad infantil en línea basado en el desarrollo

La infancia como una fase de la vida diferenciada y protegida

El reconocimiento de la infancia como una fase de la vida diferenciada es un fenómeno relativamente reciente. A lo largo de gran parte de la historia, no se consideró que los niños fueran fundamentalmente diferentes de los adultos.

En las sociedades premodernas y las primeras sociedades industriales, este punto de vista estaba estrechamente vinculado a condiciones materiales, en particular a la «necesidad económica» del trabajo infantil. La caracterización de los niños como «pequeños adultos»⁰¹ ocultaba sus necesidades y vulnerabilidades específicas, lo que impedía el desarrollo de marcos de protección infantil.

Con el auge de disciplinas científicas modernas, como la medicina del desarrollo y la psicología, se produjo un cambio de paradigma. Las pruebas demostraron que el desarrollo cognitivo, emocional y social de los niños sigue trayectorias distintas. Estos avances ayudaron a redefinir la infancia como una fase de la vida diferenciada y vulnerable⁰².

Esta idea se vio reforzada por los conocimientos aportados por la psiquiatría infantil y adolescente, que pusieron de relieve las consecuencias a largo plazo de las adversidades experimentadas en los primeros años de vida. Poco a poco, se fue afianzando la idea de que la infancia y la adolescencia son fases de la vida diferenciadas que requieren protección y apoyo⁰³.

El desarrollo infantil por etapas

A lo largo del siglo XX, esta creciente concienciación sentó las bases para unos marcos modernos de protección de la infancia y la juventud. Inicialmente, estos marcos se centraron en la protección de los niños en el mundo físico.

La Convención de las Naciones Unidas sobre los Derechos del Niño es un ejemplo clave. En virtud de la Convención, los niños menores de dieciocho años^a se consideran un grupo homogéneo.

A pesar del rápido desarrollo de las tecnologías y servicios digitales, como los medios sociales y otros servicios digitales, y de las formas en que han transformado la vida de los niños, muchos enfoques de la protección infantil siguen basándose implícita o explícitamente en la idea de «niños» como grupo homogéneo.

Esta suposición es engañosa. La ciencia del desarrollo demuestra que el desarrollo de los niños se produce en etapas cualitativamente distintas, cada una de las cuales se caracteriza por capacidades cognitivas, emocionales y sociales únicas. Estas capacidades determinan la forma en que los niños perciben sus entornos, interactúan con ellos y se comunican en ellos, también en línea.

La necesidad de una protección adaptada a la edad

«Una protección adecuada en función del desarrollo reconoce que el control cognitivo, la regulación emocional y la conciencia de los riesgos de los niños aún se encuentran en fase de maduración.»

— PROF. DRA. EVA MÖHLER
PRESIDENTA Y DIRECTORA MÉDICA DE
PSIQUIATRÍA INFANTIL Y ADOLESCENTE
DEL HOSPITAL UNIVERSITARIO DEL SARRE

La exposición de los niños al mundo de los y otros servicios digitales comienza a una edad temprana y va aumentando de forma constante a lo largo de la infancia en cuanto a intensidad, complejidad y personalización⁰⁴. Un estudio revela que los niños menores de dos años pasan una media de cuarenta y nueve minutos al día frente a las pantallas. A la edad de ocho años, esta cifra se ha triplicado con creces, hasta situarse en unas tres horas al día⁰⁵. Las pruebas muestran que las tecnologías digitales tienen un efecto generalizado y estructurador en el desarrollo de los niños y forman parte del complejo entorno en el que los niños y adolescentes aprenden, desarrollan un sentido de identidad y se relacionan con los demás.

En pocas palabras, el desarrollo de los niños influye en sus interacciones en línea y, al mismo tiempo, se ve influido por ellas. Así pues, el mundo digital no puede considerarse algo ajeno al desarrollo de los niños, sino más bien una parte fundamental del

mismo, especialmente en las etapas posteriores⁰⁶. Esta interacción bidireccional subraya la necesidad de adoptar medidas adaptadas a la edad destinadas a proteger y empoderar a los niños para que naveguen en línea con seguridad y confianza.

a. Según la Convención, se entiende por niño «todo ser humano menor de dieciocho años de edad», salvo que la mayoría de edad se alcance antes en virtud de la ley aplicable. Véase: Naciones Unidas (1989). [Convención sobre los Derechos del Niño](#). Parte 1, artículo 1.

Principales retos para una protección adaptada a la edad

LA TENDENCIA A CONSIDERAR A LOS «NIÑOS»

COMO UN ÚNICO GRUPO

Los enfoques existentes en materia de seguridad infantil en línea a menudo se basan en la idea que los niños son un único grupo con necesidades uniformes. Esta idea debe actualizarse. Hoy en día se entiende que el desarrollo infantil se produce en etapas, que determinan la forma en que los niños (de 0 a 12 años) y los adolescentes (de 13 a 18 años) interactúan con el mundo en línea y sus vulnerabilidades a diversos riesgos.

Los factores sociales, el género y la sexualidad, el contexto socioeconómico, el origen racial y étnico, la religión, el origen migrante y las necesidades educativas especiales también tienen un impacto importante en las interacciones y vulnerabilidades de los niños y adolescentes en línea⁰⁷.

EL DESAJUSTE ENTRE LAS CAPACIDADES DE LOS MENORES

Y LOS MEDIOS SOCIALES Y OTROS SERVICIOS DIGITALES

Los servicios digitales, incluidos los medios sociales, ofrecen un flujo rápido y constante de información mediante arquitecturas de interacción altamente optimizadas, incluidos los sistemas de recomendación algorítmica y el desplazamiento infinito por la pantalla. Estas funciones están diseñadas específicamente para captar al máximo la atención de los usuarios⁰⁸.

Las capacidades de los niños y adolescentes, en cambio, se desarrollan de forma gradual y siguen sin estar completas hasta bien entrada la adolescencia⁰⁹. Como consecuencia de ello, los menores están cada vez más expuestos a entornos y contenidos de medios sociales y otros servicios digitales con los que no están preparados para interactuar y que pueden causarles daños graves.

LA EVOLUCIÓN DE LA AUTONOMÍA DE LOS MENORES

COMO USUARIOS EN LÍNEA

Como se ha mencionado anteriormente y se estudia con mayor detalle en las secciones siguientes, la evolución de las capacidades de los niños y adolescentes a lo largo de su desarrollo determina (en parte) hasta qué punto están preparados para navegar en línea con seguridad y confianza a diferentes edades.

A medida que los niños crecen, pasan de depender por completo de sus progenitores y cuidadores a alcanzar una autonomía parcial y, en última instancia, convertirse en adultos totalmente autónomos. El diseño de los medios sociales y otros servicios digitales tiene una influencia cada vez mayor en el desarrollo de los menores. A medida que los niños crecen y se vuelven más independientes, las capacidades de su red de apoyo (progenitores, cuidadores, profesores y educadores) para protegerlos, supervisarlos y orientarlos en línea son más limitadas.

RECOMENDACIONES

Diseñar y desplegar medidas en línea de protección de la infancia adaptadas a la edad

El desarrollo por etapas de niños y adolescentes exige el diseño y el despliegue de medidas de protección que se adapten a la evolución de sus capacidades y que aborden los riesgos a los que están expuestos a diferentes edades. Estas medidas deben tener en cuenta, cuando sea posible, las circunstancias personales y sociales de los menores.

Garantizar espacios en línea seguros para los menores

Los proveedores de medios sociales y otros servicios digitales tienen la responsabilidad primordial de garantizar que sus servicios sean seguros para todos los niños y adolescentes. Esto incluye la implantación de características de diseño seguras. Los proveedores deben asumir la responsabilidad principal de garantizar que sus servicios sean seguros para que los menores puedan acceder a ellos y utilizarlos.

Empoderar a los menores y sus círculos de apoyo

Para que resulten eficaces, las medidas destinadas a proteger y empoderar a los niños y adolescentes en línea deben tener en cuenta la evolución de sus necesidades y capacidades. Las medidas también deben adaptarse para apoyar el papel cambiante de los progenitores, cuidadores, profesores y educadores (círculos de apoyo) a la hora de proteger a los menores y supervisar y orientar su uso de los medios sociales y otros servicios digitales a medida que crecen.

Retos específicos por edad

En la sección anterior se analizaron tres retos principales y se formularon recomendaciones complementarias destinadas a orientar el diseño y la aplicación de un enfoque de la seguridad infantil en línea basado en el desarrollo.

Sobre esta base, en las siguientes secciones se analizan las diversas características y vulnerabilidades que definen el desarrollo de los menores a lo largo de tres etapas primarias de su desarrollo: 0-2 años (primera infancia); 3-12 años (infancia); y 13-18 años (adolescencia).

Estas etapas primarias abarcan tanto la evolución de las capacidades de los menores como el papel cambiante de sus círculos de apoyo a la hora de proteger y empoderar a los niños y adolescentes en línea:

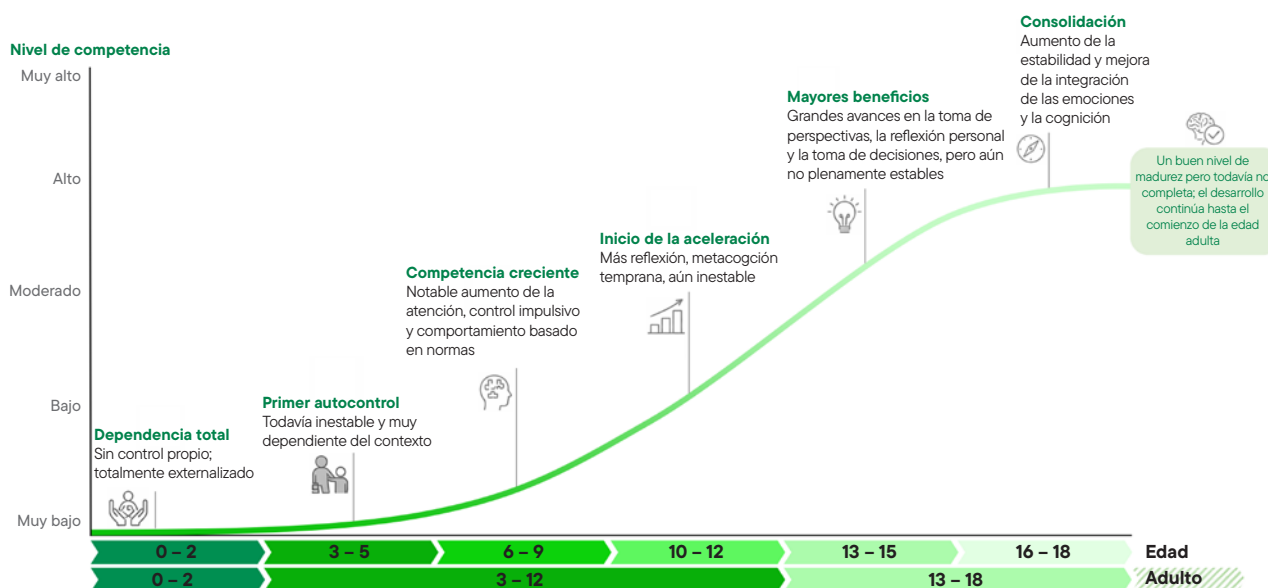
// **0-2 años:** la primera infancia como etapa de desarrollo especialmente protegida;

// **3-12 años:** la infancia como etapa de desarrollo supervisada;

// **13-18 años:** la adolescencia como etapa de autonomía progresiva.

Gráfico 1. El desarrollo por etapas de las competencias básicas

Autorregulación, criterio y pensamiento crítico



En el presente informe se examinan los riesgos a los que se enfrentan los menores en línea y se presentan recomendaciones para abordarlos en función de estas tres etapas primarias del desarrollo, definidas a efectos de este análisis como primera infancia, infancia y adolescencia.

En este primer capítulo se expone el primero de los seis principios rectores propuestos por los autores para orientar las medidas destinadas a proteger y empoderar a los niños y adolescentes en el mundo digital: la necesidad de un enfoque de la seguridad infantil en línea basado en el desarrollo.

A fin de garantizar un examen exhaustivo de las características y vulnerabilidades específicas de los menores en las distintas etapas de su desarrollo, las etapas primarias se dividen en etapas secundarias (0-2 años, 3-5 años, 6-9 años, 10-12 años, 13-15 años y 16-18 años), que se analizan en profundidad en este capítulo.

Algunas de las recomendaciones presentadas para cada etapa primaria no son exclusivas de la etapa en la que se sitúan, sino que se aplican a todas las etapas, tal como se especifica.

0-2 años: la primera infancia como etapa de desarrollo especialmente protegida

La primera infancia, en particular de 0 a 2 años, constituye una etapa de máxima dependencia e importancia fundamental para el desarrollo. Durante este período, se establecen los pilares fundamentales de la seguridad emocional, la conexión social, la adquisición del lenguaje y la autorregulación.

Los procesos básicos, como la formación del apego, la correulación y la diferenciación entre el yo y el entorno del niño, surgen a través de interacciones repetidas con cuidadores receptivos. La autorregulación aún no está consolidada internamente, sino que se desarrolla de forma gradual a través de la correulación.

«Todas las personas menores de 18 años tienen derechos específicos a la protección y al disfrute de experiencias adecuadas a su edad.»

— MIE OEHLENSCHLAGER,
INVESTIGADORA INDEPENDIENTE EN IA,
ÉTICA Y POLÍTICAS PÚBLICAS

En este sentido, la corregulación temprana también constituye la base del desarrollo para una autonomía posterior y un funcionamiento autodeterminado. La interiorización gradual de la regulación emocional, la comunicación y la interacción social se produce a través de experiencias relacionales repetidas, más que mediante una exposición aislada a los estímulos digitales.

El desarrollo durante esta etapa es fundamentalmente relacional. Las capacidades de autorregulación, la estabilidad emocional y las primeras estructuras cognitivas se apoyan en factores externos antes de ser interiorizadas.

RETOS ESPECÍFICOS POR EDAD

La necesidad de interacción humana directa

Un reto fundamental en esta etapa es garantizar que los niños pequeños tengan suficiente interacción humana directa. La reducción de la calidad de la interacción puede afectar a los procesos de apego y dificultar el desarrollo temprano del lenguaje y las capacidades comunicativas fundamentales, lo que repercute directamente en las trayectorias de desarrollo.

Garantizar la disponibilidad de interacciones coherentes y en sintonía con las emociones constituye una condición básica para un desarrollo seguro en entornos cada vez más digitalizados. Durante esta etapa, los niños pequeños dependen casi por completo de la regulación externa.

Los sistemas neurofisiológicos que intervienen en la regulación del estrés, la modulación de la activación y los ciclos de sueño y vigilia aún son inmaduros y muy sensibles a los estímulos ambientales. Esto genera una mayor vulnerabilidad a la sobreestimulación y a las alteraciones del sueño y de la regulación del estrés.

El aprendizaje en esta etapa se basa en la interacción, más que en el contenido. Los niños pequeños construyen significados mediante una interacción corporal y recíproca con sus progenitores y cuidadores, no mediante una exposición pasiva a representaciones en pantalla.

La adquisición temprana del lenguaje y el desarrollo de la comunicación dependen fundamentalmente de la interacción reiterada y contingente con los progenitores y cuidadores. La interacción verbal receptiva, la atención compartida y la comunicación en sintonía con las emociones constituyen condiciones esenciales para el desarrollo durante esta etapa.

Riesgos de la exposición a las pantallas

A esta edad, las pruebas relacionan una mayor exposición a las pantallas con una menor duración del sueño, patrones desregulados de respuesta al estrés y menores niveles de interacción entre los cuida-

dores y los niños y de exposición a estímulos lingüísticos¹⁰. Estas vulnerabilidades pueden distinguirse en los planos biológico, psicológico y de desarrollo.

Desde el punto de vista biológico, los niños pequeños son muy vulnerables a la sobreestimulación debido a la inmadurez de sus sistemas de autorregulación¹¹. Desde el punto de vista psicológico, el desarrollo depende de una interacción constante y receptiva, que hace que los niños pequeños sean sensibles a las alteraciones en la atención y la comunicación. Desde el punto de vista del desarrollo, los riesgos están relacionados con la formación del apego y la aparición de la autorregulación.

Durante esta etapa, una mayor exposición a las pantallas se ha asociado con dificultades socioemocionales, problemas de conducta y retrasos en el desarrollo de la autorregulación¹². Estas relaciones suelen ser bidireccionales, ya que los niños pequeños con dificultades de autorregulación también pueden pasar más tiempo frente a las pantallas.

Exposición digital mediada por los cuidadores

De 0 a 2 años, la exposición a los medios sociales y otros servicios digitales está totalmente mediada por los cuidadores. En principio, los niños pequeños no controlan el acceso, la duración ni el contenido. El uso de los medios sociales y otros servicios digitales está determinado principalmente por las prácticas, rutinas y necesidades situacionales de los progenitores y cuidadores, como calmar o distraer al niño¹³.

Durante la primera infancia, los riesgos digitales surgen, en teoría, no tanto de la interacción directa con los contenidos, sino más bien de la forma en que los medios sociales y otros servicios digitales reestructuran los entornos de cuidado. Un concepto fundamental es la «tecnointerferencia»^b. A esta edad, incluso los cambios breves en la atención del cuidador pueden reducir la capacidad de respuesta, la atención conjunta y la interacción verbal¹⁴.

El uso de pantallas por parte de los cuidadores en presencia de niños pequeños se ha asociado con resultados de desarrollo menos favorables. Esto no se debe principalmente al contenido, sino a la reestructuración del espacio de interacción¹⁵. En este sentido, el riesgo digital en la primera infancia suele ser relacional antes que individual.

Las investigaciones sobre los influyentes que muestran su vida familiar con fines comerciales ponen de relieve que los niños pequeños pueden convertirse cada vez más en objetos de visibilidad, monetización y extracción de datos mucho antes de que puedan comprender o influir ellos mismos en estos procesos. Esto refuerza la necesidad de contar con marcos de protección externos sólidos durante la primera infancia.

La digitalización de la primera infancia

Una dimensión emergente y cada vez más pertinente se refiere a la digitalización de los entornos de la primera infancia más allá de las interacciones tradicionales basadas en pantallas. Un número cada vez mayor de juguetes, como muñecas y objetos de juego interactivos, se equipan con funciones digitales y, cada vez más, con inteligencia artificial (IA).

b. La «tecnointerferencia» se define como la interrupción de la interacción entre progenitores e hijos por la tecnología. Véase: Zhang et al. (2025). *Parental Technoference and Child Problematic Media Use: Meta-Analysis* [«Tecnointerferencia parental y uso problemático de los medios digitales por parte de los niños: metanálisis», documento en inglés].

Esta evolución hacia un entorno de medios sociales y otros servicios digitales resulta especialmente pertinente, ya que los juguetes dotados de IA y los dispositivos basados en la voz pueden ser percibidos por los niños no solo como objetos, sino como interlocutores sociales capaces de responderles. Durante la primera infancia, el apego, la corregulación, la adquisición del lenguaje y el juego simbólico dependen de una interacción humana contingente.

Estos sistemas plantean problemas específicos en términos de desarrollo. Los juguetes dotados de IA y los dispositivos basados en la voz pueden simular la capacidad de respuesta sin ofrecer la reciprocidad auténtica, la sintonía emocional ni la responsabilidad relacional que caracterizan a las relaciones humanas.

Los juguetes dotados de IA también suelen integrar micrófonos, cámaras, procesamiento del habla o personalización basada en aplicaciones. Esto conlleva riesgos para la privacidad y la protección de datos a una edad en la que los niños no tienen capacidad para comprender, dar su consentimiento o impugnar el tratamiento de datos.

Sustitución de la interacción humana directa

Las interacciones de los niños con el mundo digital suscitan preocupación por una posible sustitución o distorsión de los procesos de aprendizaje interactivo, así como por nuevas formas de dependencia y sobreestimulación. Estas dependencias aún no se han abordado de forma adecuada en las investigaciones existentes ni en los marcos reglamentarios vigentes.

El uso de los medios sociales y otros servicios digitales por parte de los progenitores y cuidadores puede reducir el tiempo dedicado a la interacción cara a cara con los niños, al juego libre, a la actividad física y al sueño, todos ellos aspectos esenciales para el desarrollo temprano¹⁶. En sus formas más graves, la sustitución de las interacciones con los cuidadores puede equivaler a una «negligencia digital»^c.

Los problemas relacionados con la sustitución de las interacciones cara a cara entre cuidadores y niños van más allá de la sobreestimulación o la distracción inmediatas y abarcan posibles efectos a largo plazo en el desarrollo de la autonomía, el juego imaginativo, la comunicación y el desarrollo de capacidades sociales y emocionales guiadas internamente.

Un enfoque muy restrictivo de la exposición digital

A pesar de estos retos, no todas las formas de uso de los medios sociales y otros servicios digitales durante la primera infancia son intrínsecamente perjudiciales. En condiciones específicas, especialmente cuando los progenitores y cuidadores se aseguran de que el contenido sea adecuado para la edad (poco estimulante, de ritmo lento, etc.) y se integre en una mediación activa por parte de los cuidadores, los espacios de los medios sociales y otros servicios digitales pueden favorecer ciertos aspectos del aprendizaje temprano.

- c. Partiendo de las formas establecidas de negligencia emocional y de supervisión (Dubowitz *et al.*, 1993; Hildyard y Wolfe, 2002), la negligencia digital amplía estos conceptos a los entornos digitales. Cuando los progenitores hacen un uso intensivo de las pantallas en presencia de sus hijos, disminuyen las interacciones y la capacidad de respuesta de los progenitores. El desarrollo del lenguaje de los niños puede verse afectado. Esta sustitución también puede generar sentimientos de rechazo y distancia emocional en los niños, lo que aumenta su riesgo de sufrir depresión, ansiedad y agresividad.

Las pruebas demuestran que la participación conjunta en los medios sociales y otros servicios digitales (uso conjunto) puede facilitar el aprendizaje, especialmente cuando va acompañada de interacción verbal y apoyo¹⁷. Sin embargo, estos efectos parecen limitados y dependen del contexto.

El mantenimiento de la interacción relacional con los niños pequeños no solo es pertinente para prevenir daños, sino también para propiciar un desarrollo socioemocional, lingüístico y cognitivo saludable. El apego seguro, la comunicación receptiva y el ejemplo de los cuidadores constituyen factores de protección fundamentales en unos entornos de cada vez más digitalizados en la primera infancia.

En conjunto, estas conclusiones respaldan un enfoque muy restrictivo del uso de los medios sociales y otros servicios digitales en la primera infancia, en consonancia con las orientaciones de las principales autoridades de salud pediátrica¹⁸. Aunque es posible que estas recomendaciones no se cumplan de forma universal, proporcionan importantes orientaciones normativas acordes con las necesidades de desarrollo de este grupo de edad.

Interacciones en línea centradas en los cuidadores

La seguridad infantil en línea durante la primera infancia debe centrarse fundamentalmente en los cuidadores. Dado que los niños pequeños no son usuarios autónomos, la responsabilidad de su exposición a los entornos digitales recae, sobre todo, en los progenitores y cuidadores.

La capacidad de mediación parental se distribuye de forma desigual. La situación socioeconómica, la salud mental de los progenitores y el propio uso que estos hacen de los medios sociales y otros servicios digitales influyen de forma significativa en los patrones de exposición de los niños [como se analiza con más detalle en el capítulo 2]. Un mayor nivel de estrés parental y un mayor uso de pantallas se asocian con un uso más prolongado y menos estructurado de los servicios digitales por parte de los niños muy pequeños¹⁹. Por tanto, se desaconseja encarecidamente el uso de pantallas para este grupo de edad.

CONCLUSIONES

La seguridad en línea durante la primera infancia no consiste principalmente en regular el comportamiento de los niños pequeños, sino en estructurar los entornos de cuidado y los contextos de interacción. La protección depende del mantenimiento de las condiciones necesarias para el apego, la corregulación y el desarrollo de la autorregulación. Estas condiciones constituyen la base para las etapas posteriores del desarrollo.

Las conclusiones extraídas de los sistemas de clasificación por edades ya establecidos (por ejemplo, las clasificaciones de películas y videojuegos) pueden servir de orientación. Si un contenido está diseñado para este grupo de edad, debe limitarse estrictamente a formatos poco estimulantes, de ritmo lento y no narrativos que favorezcan la participación conjunta con los cuidadores. Esto incluye estímulos visuales o auditivos sencillos integrados en contextos de uso conjunto.

Los contenidos de ritmo rápido, altamente estimulantes o que provocan emociones intensas, como los cambios rápidos de escena, los efectos audiovisuales intensos o las narrativas con una fuerte carga emocional, deben considerarse inadecuados desde el punto de vista del desarrollo. La exposición a cualquier forma de contenido narrativo complejo, violento o aterrador es claramente inadecuada a esta edad.

RECOMENDACIONES (0-2 AÑOS)

Aumentar la concienciación de los cuidadores sobre la importancia para el desarrollo de la interacción humana directa, desde la primera infancia

Empoderar a los progenitores y cuidadores mediante campañas educativas y programas de apoyo a la crianza sobre la importancia de la primera infancia para el desarrollo de los niños. Informar a los cuidadores sobre los riesgos para los niños pequeños asociados a la «tecnointerferencia», por ejemplo, el uso que los propios cuidadores hacen de los medios sociales y otros servicios digitales. Animar a los cuidadores a reflexionar sobre los efectos directos e indirectos de sus interacciones en línea en los menores de todas las edades, especialmente los niños pequeños.

Los riesgos de «negligencia digital» deben reconocerse en los marcos de protección infantil. Los progenitores, las escuelas y los servicios sociales deben recibir información sobre cómo detectar los signos de negligencia digital en niños y adolescentes, desde la primera infancia.

Evitar las pantallas y los medios sociales y otros servicios digitales para los niños menores de 3 años

Durante los primeros mil días de vida, las necesidades de desarrollo de los niños están relacionadas principalmente con el apego, la correulación, el desarrollo sensorial y la adquisición temprana del lenguaje. Sin embargo, evitar la exposición a los medios sociales y otros servicios digitales y pantallas durante la primera infancia no implica una prohibición absoluta.

En condiciones específicas, los medios sociales y otros servicios digitales pueden utilizarse de forma relacional y limitada con niños pequeños, por ejemplo, como parte de actividades compartidas (como ver fotos familiares o comunicarse con familiares a través de videollamadas). No obstante, debe evitarse estrictamente el uso de pantallas como herramientas para «calmar» u ocupar a los niños pequeños durante períodos prolongados.

Como principio general, los progenitores y cuidadores deben dar prioridad a las interacciones cara a cara con los niños y adolescentes (desde la primera infancia) para favorecer el desarrollo cognitivo, físico y emocional saludable de los menores.

Limitar la difusión de datos de niños a través de perfiles de medios sociales

Los marcos reglamentarios deben abordar la documentación sistemática y la difusión pública de los datos de los niños (incluidas imágenes y vídeos), especialmente en lo que respecta a los niños menores de 3 años, a través de perfiles de medios sociales (por ejemplo, mediante la «sobrexposición de los hijos» y los «influyentes que muestran su vida familiar»). Los niños de esta edad carecen de capacidad para dar su consentimiento a su representación digital o para comprender los contextos comerciales en los que se utilizan sus datos y las repercusiones futuras.

Los proveedores de medios sociales y otros servicios digitales no deben incentivar la creación o difusión de contenidos en los que aparezcan niños mediante estructuras de monetización, amplificación algorítmica o características de diseño orientadas a fomentar la interacción. Deben establecerse obligaciones exigibles para los medios sociales y otros servicios digitales, en lugar de confiar únicamente en la responsabilidad voluntaria de los cuidadores. Los cuidadores deben recibir orientaciones claras sobre las repercusiones a largo plazo de la visibilidad digital temprana para la privacidad, la dignidad y el derecho a la autodeterminación informativa de los niños.

3-12 años: la infancia como etapa de desarrollo supervisada

3-5 AÑOS: LA ETAPA DE DESARROLLO BAJO

UNA SUPERVISIÓN ESTRICTA

Entre los 3 y los 5 años, los niños entran en una etapa de desarrollo caracterizada por actividades intencionales bajo una estructuración externa continua. Los niños empiezan a desarrollar la capacidad de actuar de forma intencional, el pensamiento simbólico y un sentido más coherente de sí mismos.

Desde el punto de vista del desarrollo neurológico, esta etapa se caracteriza por la maduración continua de los sistemas implicados en la atención, la función ejecutiva y la regulación emocional, que siguen siendo incompletos y sensibles a la estimulación externa²⁰. Sin embargo, los sistemas relacionados con la recompensa ya están activos. Los niños desarrollan cada vez más la motivación intrínseca, la exploración impulsada por la curiosidad y las primeras formas de comportamiento autónomo orientado a objetivos.

El desarrollo durante esta etapa depende en gran medida de las oportunidades de juego imaginativo, actividades iniciadas por iniciativa propia y experiencias relacionales que favorezcan el desarrollo de competencias. Esto incluye la formación de un yo narrativo, expresado, por ejemplo, a través del lenguaje y los juegos de rol.

Los niños de esta edad pueden realizar actividades durante períodos limitados, pero su capacidad para regular la atención, los impulsos y las emociones sigue dependiendo en gran medida del apoyo externo en forma de lenguaje, imitación y orientación por parte de los cuidadores. Por lo tanto, esta etapa puede entenderse como una transición de la correulación a la autorregulación guiada.

RETOS ESPECÍFICOS POR EDAD

Vulnerabilidad a la gratificación inmediata

Esta brecha entre la maduración aún en curso de los sistemas implicados en la atención, la función ejecutiva y la regulación emocional de los niños y los sistemas de recompensa que ya están activos genera un desequilibrio. Los niños de esta edad son muy sensibles a los estímulos llamativos y a las recompensas inmediatas, pero tienen un control inhibitorio y una tolerancia a la demora limitados.

Esto hace que los niños de entre 3 y 5 años sean especialmente vulnerables a los entornos de medios sociales y otros servicios digitales optimizados para la gratificación inmediata, la recompensa repetitiva y la estimulación externa continua. Las pruebas experimentales indican que los entornos digitales pueden interferir en el desarrollo de la tolerancia a la frustración, la perseverancia y la motivación guiada internamente²¹.

Esta configuración del desarrollo crea un perfil de vulnerabilidad específico. El condicionamiento de los sistemas de recompensa mediante la respuesta rápida, la repetición y el refuerzo intermitente que se produce en las interacciones en línea de los niños puede configurar expectativas de gratificación inmediata y contribuir al desarrollo de patrones de uso habituales²².

La dependencia excesiva de estructuras de recompensa externas también puede afectar al desarrollo de la motivación intrínseca. El uso de tecnologías digitales por parte de los niños, caracterizado por el refuerzo continuo y la respuesta inmediata, puede orientar el comportamiento hacia patrones de interacción regulados externamente, en lugar de hacia la exploración y el aprendizaje impulsados por la motivación interna.

Esto reviste especial importancia durante las etapas del desarrollo en las que la autonomía y la competencia aún se están forjando. Las investigaciones indican que estas vulnerabilidades se ven muy influenciadas por factores contextuales, como el entorno familiar, la mediación parental y las condiciones socioeconómicas²³.

Riesgos de la exposición a las pantallas

Unos niveles más elevados de exposición a las pantallas en esta etapa se asocian con una menor autorregulación, en particular en lo que respecta a la atención y el control de los impulsos de los niños²⁴. Como se ha examinado anteriormente, el uso de los medios sociales y otros servicios digitales puede sustituir actividades críticas para el desarrollo, como el juego libre, la actividad física, el sueño y la interacción cara a cara²⁵.

Sin embargo, estos efectos dependen del contexto y se ven influidos por la calidad de los contenidos, el uso conjunto, el momento y el entorno social, más que por parámetros como el tiempo frente a las pantallas por sí solo²⁶. Las pruebas indican que las interacciones en línea a esta edad pueden favorecer el aprendizaje cuando el contenido es interactivo, adecuado a la edad y se integra en la mediación activa por parte de los cuidadores²⁷.

La disponibilidad de alternativas seguras fuera de línea

La seguridad infantil en línea no puede entenderse plenamente sin tener en cuenta el entorno más amplio de la vida cotidiana de los niños. En contextos en los que las oportunidades educativas, recreativas y sociales para los niños son limitadas, en particular en zonas rurales o insuficientemente atendidas, los entornos de los medios sociales y otros servicios digitales pueden convertirse en los espacios de interacción por defecto.

Esto puede exponer a los niños a daños y afectar negativamente a su desarrollo. A fin de limitar los posibles efectos nocivos del uso de los medios sociales y otros servicios digitales en el desarrollo de los niños, los progenitores y cuidadores deben ofrecer alternativas seguras fuera de línea desde la primera infancia. Más allá de los cuidadores, las condiciones estructurales y ambientales fuera de la esfera digital

configuran los patrones de exposición y los riesgos asociados. Entre ellas figuran el acceso a espacios públicos seguros, actividades extracurriculares e infraestructuras sociales de apoyo.

Reducción de la capacidad de mediación de los cuidadores

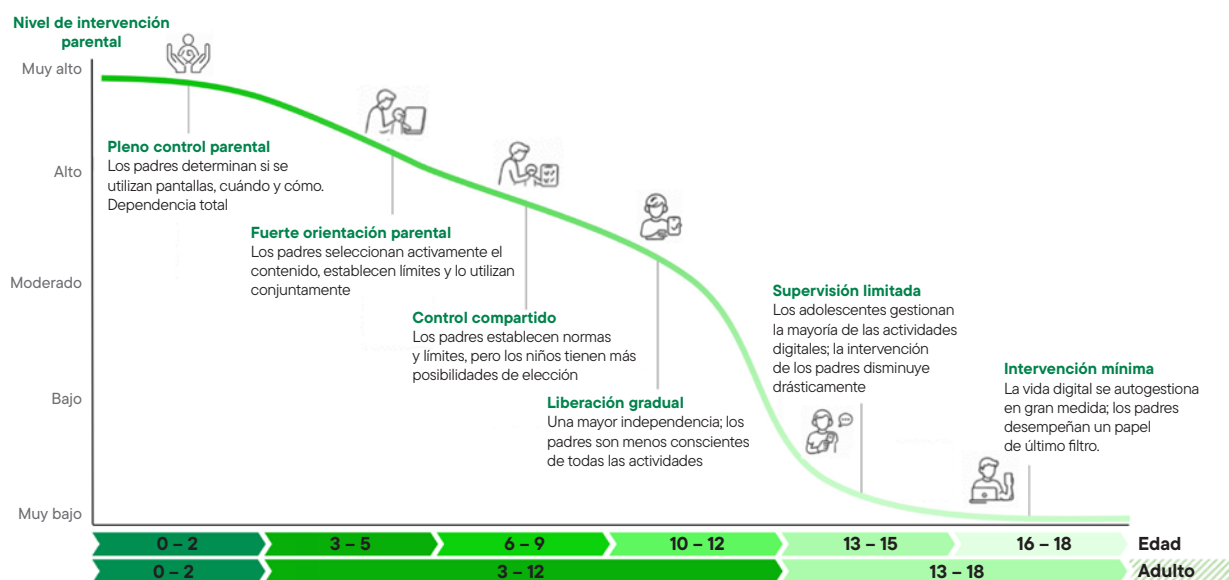
Entre los 3 y los 5 años, la mediación de los cuidadores sigue siendo un mecanismo regulador fundamental, pero experimenta un cambio cualitativo. Los progenitores y cuidadores pasan del control directo a la mediación supervisada, el uso conjunto y el apoyo interpretativo.

Las actividades iniciadas cada vez más por los propios niños reducen la eficacia de un control puramente externo, ya que la influencia parental compite con sistemas digitales muy atractivos. Las herramientas de control parental existentes a menudo no apoyan adecuadamente este cambio, por ejemplo, debido a su fragmentación entre distintos espacios de medios sociales y otros servicios digitales y a su escasa facilidad de uso²⁸.

Se ha demostrado que la mediación activa —debatir el contenido, estructurar el uso y proporcionar explicaciones— favorece el aprendizaje y mitiga los riesgos. Las estrategias puramente restrictivas pueden resultar menos eficaces sin este tipo de interacción²⁹. La mediación de los cuidadores también se ve limitada por factores como la alfabetización digital, los recursos socioeconómicos, el estrés parental y el uso que los propios cuidadores hacen de los servicios digitales³⁰.

Gráfico 2. La disminución de la mediación parental a lo largo del desarrollo

A medida que los niños crecen, la supervisión parental directa disminuye de forma natural, junto con la dependencia digital de los niños



CONCLUSIONES

Esta etapa representa una transición crítica para la seguridad infantil en línea. Los niños ya no son receptores pasivos de los contenidos a los que se ven expuestos, sino participantes cada vez más activos en el mundo digital, aunque aún carecen de una autorregulación estable. La exposición se amplía, mientras que la regulación interna sigue siendo incompleta.

Mientras tanto, la responsabilidad comienza a pasar del control puramente parental a un sistema más amplio en el que participan las familias y las instituciones educativas. Desde una perspectiva estratégica, esto implica un papel reducido, pero importante, de la supervisión parental. El principal reto a esta edad no es simplemente limitar la exposición, sino evitar la consolidación de patrones de uso nocivos a una edad temprana.

Las medidas de protección infantil en línea para este grupo de edad deben incluir un apoyo ambiental e institucional estructurado. Esto incluye un diseño de las aplicaciones y los contenidos digitales dirigidos a los niños de corta edad que sea adecuado para su edad, prestando especial atención a los mecanismos basados en recompensas y destinados a captar la atención.

Dado el aumento gradual de las actividades iniciadas por los propios niños a partir de esta edad, la educación digital debe integrarse en la educación de la primera infancia. A la luz del papel de supervisión que siguen desempeñando los cuidadores, deben reforzarse la orientación parental y las prácticas de uso conjunto, especialmente en contextos vulnerables.

Los marcos reglamentarios actuales a menudo pasan por alto esta etapa de desarrollo y se centran en los niños muy pequeños o en los adolescentes. Como consecuencia de ello, las vulnerabilidades específicas de los niños de entre 3 y 5 años siguen sin abordarse de manera suficiente. La seguridad infantil en línea a esta edad debe centrarse en el diseño de entornos que favorezcan, en lugar de socavar, el desarrollo de la autorregulación de los niños y que empoderen a los cuidadores para supervisar el uso que hacen los niños de estos entornos.

6-9 AÑOS: LA ETAPA DE DESARROLLO BAJO SUPERVISIÓN

Entre los 6 y los 9 años, los niños entran en una etapa de desarrollo caracterizada por una competencia cognitiva cada vez mayor, un comportamiento estructurado y orientado a objetivos y la aparición de la autoevaluación basada en las competencias. Los niños ahora son capaces de participar de forma más constante en actividades regidas por normas, mantener la atención durante períodos más largos y perseguir objetivos definidos.

Una tarea central del desarrollo es la formación de un sentido de identidad basado en la competencia, en el que la autoestima se vincula cada vez más al desempeño y a la valoración externa. Durante esta etapa, el desarrollo de la competencia y la autoeficacia adquiere una importancia cada vez mayor para un desarrollo psicológico saludable. Los niños desarrollan una autorregulación más estable, aprenden gradualmente a tolerar la frustración y persisten en tareas difíciles.

Además, los niños empiezan a obtener satisfacción del dominio y de la sensación interna de competencia, más que únicamente de las recompensas externas inmediatas. Con el inicio de la escolarización, los sistemas estructurados de evaluación y la comparación con los compañeros pasan a ocupar un lugar central y determinan la forma en que los niños interpretan sus capacidades en relación con criterios externos.

Desde el punto de vista neurobiológico, esta etapa se caracteriza por una mayor eficiencia y especialización de las redes cerebrales, en particular en las regiones asociadas al funcionamiento ejecutivo. Sin embargo, los sistemas de recompensa y estrés siguen siendo sensibles, lo que da lugar a una configuración en la que los niños son más capaces de autorregularse, pero siguen respondiendo al refuerzo externo.

RETOS ESPECÍFICOS POR EDAD

Mayor sensibilidad a la evaluación externa

Los entornos de los medios sociales y otros servicios digitales se entrecruzan directamente con estos procesos. Los medios sociales y otros servicios digitales que proporcionan valoraciones cuantificables, como puntuaciones, clasificaciones y logros, están claramente en consonancia con una autoevaluación basada en las competencias.

Esto puede influir en la motivación y la autopercepción al imponer criterios externos de éxito³¹ en lugar de la experiencia interna de dominio, la curiosidad y los procesos de aprendizaje. A esta edad, los sistemas de atención siguen siendo sensibles a los entornos muy estimulantes, que pueden competir con la atención sostenida necesaria para el aprendizaje³².

Riesgo de adicción temprana

Entre los 6 y los 9 años, los hábitos de los niños se estabilizan, a medida que los patrones de uso de los medios sociales y otros servicios digitales, la atención y la motivación se vuelven más constantes con el tiempo. A esta edad, el refuerzo basado en recompensas, especialmente en los videojuegos, puede contribuir a la formación de patrones de uso habituales³³. Estas vulnerabilidades vienen determinadas por factores contextuales, como el entorno familiar, la mediación parental y las condiciones socioeconómicas³⁴.

Durante estos años, el acceso de los niños a los medios sociales y otros servicios digitales se amplía considerablemente. Con el inicio de la escolarización y el aumento de la interacción con los compañeros, los niños obtienen un acceso más frecuente y menos supervisado a los espacios de los medios sociales y otros servicios digitales. Esta expansión va acompañada de una disminución gradual del control parental directo, aunque la supervisión de los cuidadores sigue siendo fundamental.

A esta edad, la mediación parental se orienta cada vez más hacia el establecimiento de normas, la supervisión y la orientación. Sin embargo, su eficacia disminuye a medida que aumentan el acceso independiente de los niños y la complejidad de los medios sociales y otros servicios digitales³⁵. La responsabilidad de configurar los entornos digitales de los niños se distribuye cada vez más entre los proveedores de medios sociales y otros servicios digitales, los cuidadores y los educadores.

Riesgos de la exposición a las pantallas

Al igual que en etapas anteriores, el uso de servicios en línea por parte de los niños puede sustituir actividades cruciales para su desarrollo en el «mundo real», como la actividad física, el sueño y las interacciones cara a cara³⁶. Un ejemplo que se debate con frecuencia es el de las escuelas primarias sin teléfonos móviles, como contrapeso deliberado a la creciente digitalización de la vida de los niños. Las investigaciones sugieren que restringir el uso de los teléfonos inteligentes durante la jornada escolar puede mejorar no solo la concentración y el rendimiento académico de los niños, sino también reforzar la interacción social.

Las revisiones de la investigación indican que los entornos sin teléfonos inteligentes pueden mejorar el bienestar social y reducir los conflictos, como el ciberacoso³⁷. Las pruebas procedentes de intervenciones a nivel sistémico, por ejemplo, en países como los Países Bajos, también sugieren que restringir el uso de teléfonos inteligentes contribuye a crear un entorno de aprendizaje más tranquilo y propicio³⁸. Los

estudios muestran de forma sistemática que los teléfonos inteligentes presentan un importante potencial de distracción en el aula y pueden perjudicar la atención de los niños³⁹.

Sin embargo, en condiciones adecuadas, el uso de servicios en línea a esta edad puede favorecer el aprendizaje y la participación cognitiva de los niños, especialmente cuando está estructurado y adaptado a su desarrollo⁴⁰. Los sistemas de tutoría adaptativa y las aplicaciones educativas pueden favorecer itinerarios de aprendizaje individualizados, proporcionar explicaciones y reducir la dependencia del apoyo de los cuidadores. Esto puede contribuir a la inclusión educativa.

CONCLUSIONES

La seguridad infantil en línea durante esta etapa requiere un enfoque multinivel. Esto implica la necesidad de establecer normas claras para un diseño de los medios sociales y otros servicios digitales adecuado a la edad, especialmente en lo que respecta a los sistemas de valoración externa y los mecanismos de recompensa que interactúan con el desarrollo de autoconceptos, la autorregulación y la motivación intrínseca de los niños. Los bucles de refuerzo y las funciones de monetización que afectan a la atención y a la motivación intrínseca requieren especial atención.

La educación digital de los niños debe reforzarse en los sistemas escolares, centrándose no solo en las competencias técnicas, sino también en la atención, la autorregulación y una participación crítica. Se necesitan marcos estructurados para el uso de servicios línea que equilibren la participación digital con las actividades fuera de línea.

La escuela primaria sin teléfonos móviles puede entenderse como un mecanismo de protección y aprendizaje adecuado para el desarrollo. Esto crea espacios en los que los niños pueden desarrollar competencias sociales esenciales, como la comunicación cara a cara, la resolución de conflictos y la interacción cooperativa. Estas competencias constituyen la base para un uso de servicios en línea más reflexivo y responsable en etapas posteriores.

Estas medidas no deben concebirse como una prohibición de las tecnologías digitales, sino como un uso de los servicios en línea integrado en la práctica pedagógica y supervisado, que refuerce las experiencias analógicas de los niños, al tiempo que los prepara gradualmente para la alfabetización mediática en entornos de medios sociales y otros servicios digitales. Estas medidas no sustituyen el papel de los progenitores o cuidadores, cuya mediación informada sigue siendo un componente central de una protección eficaz.

10-12 AÑOS: LA ETAPA DE DESARROLLO

CON UNA SUPERVISIÓN CADA VEZ MENOR

Las edades comprendidas entre los 10 y los 12 años constituyen una etapa crítica del desarrollo de los niños, caracterizada por una reorganización del yo en relación con los demás. El concepto del yo se vuelve más diferenciado, pero también más inestable, a medida que los niños construyen cada vez más su identidad a través de la comparación con sus compañeros, el posicionamiento social y la aceptación percibida. Paralelamente, la valoración externa se convierte en un principio organizativo central de la autoevaluación.

Las relaciones con los compañeros adquieren una importancia considerable. Los compañeros actúan cada vez más como puntos de referencia fundamentales en cuanto a normas, valores y comportamientos.

Los procesos de influencia social, como la presión de conformidad, la comparación social y las normas implícitas del grupo, moldean de manera significativa la autopercepción y el comportamiento de los niños.

Las redes de compañeros desempeñan importantes funciones de apoyo. Proporcionan validación emocional, orientación social y oportunidades para afrontar juntos los retos del desarrollo. El apoyo de los compañeros puede actuar como fuente de resiliencia y como amplificador de las dinámicas de riesgo, dependiendo del contexto y de las normas imperantes en el grupo.

RETOS ESPECÍFICOS POR EDAD

Acceso continuo a los servicios en línea

Con la edad, estos procesos entre iguales se trasladan cada vez más a entornos digitales. Los medios sociales y otros servicios digitales permiten una interacción continua, de fácil acceso y, a menudo, sin límites entre los niños y sus compañeros. Esto permite establecer y mantener la conexión social y el sentido de pertenencia más allá de los contextos físicos.

Para muchos niños de esta edad, el acceso a los medios sociales y otros servicios digitales ya se convierte en un requisito previo para la participación social. Al igual que en la etapa anterior, el uso de los medios sociales y otros servicios digitales puede sustituir actividades cruciales para el desarrollo, como la actividad física, el sueño y la interacción fuera de línea⁴¹.

Intensificación de la comparación social

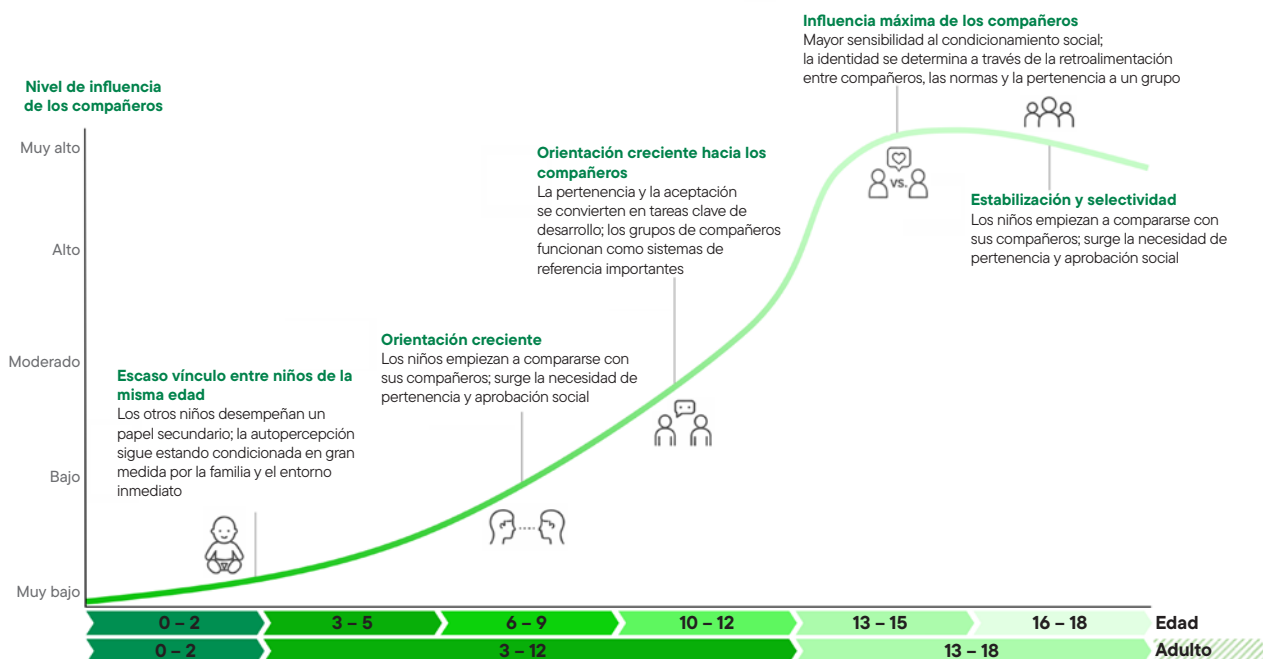
Las características estructurales de los medios sociales y otros servicios digitales, especialmente la persistencia, visibilidad y escalabilidad de las interacciones, intensifican los efectos de la influencia de los compañeros. Los entornos estructurados algorítmicamente también pueden amplificar estas dinámicas al priorizar de forma continua contenidos con una fuerte carga emocional, socialmente gratificantes o muy atractivos.

A esta edad, los niños se evalúan cada vez más a sí mismos en distintos ámbitos, como la apariencia, la popularidad y la competencia social. También empiezan a presentar de forma intencional una determinada imagen de sí mismos y a experimentar con su identidad, especialmente en los entornos digitales.

Otro mecanismo tiene que ver con la interiorización de normas y comportamientos. La exposición a contenidos que muestran comportamientos de riesgo o normas perjudiciales puede aumentar la probabilidad de imitación, sobre todo durante una etapa en la que los marcos normativos aún se están formando⁴². Los riesgos más graves, como la coacción o la explotación, son menos frecuentes, pero potencialmente más perjudiciales.

Gráfico 3. El aumento de la influencia de los compañeros a lo largo del desarrollo

A medida que los niños crecen, la influencia de los compañeros aumenta y alcanza su punto álgido durante la adolescencia, cuando el sentido de pertenencia, la evaluación social y la expresión de la identidad pasan a ocupar un lugar central.



Influencia de los algoritmos en la formación de la identidad

En una etapa de desarrollo marcada por la formación incipiente de la identidad y una mayor orientación hacia los compañeros, la amplificación algorítmica también puede contribuir a configurar la formación de opiniones, la orientación social y la autoevaluación de maneras que los niños aún no son capaces de reconocer ni resistir por completo.

Las plataformas de medios sociales y otros servicios digitales proporcionan herramientas para construir la identidad y gestionar la impresión que se proyecta ante los demás⁴³. La identidad en línea no solo se experimenta, sino que se muestra y evalúa continuamente, lo que crea un nuevo contexto de desarrollo. Para los niños de esta edad, la visibilidad en los medios sociales se convierte en una dimensión significativa de su situación entre los compañeros⁴⁴.

Los niños interactúan cada vez más con entornos de información personalizados en los que los contenidos se seleccionan en función del grado de interacción previsto, en lugar de su adecuación a la etapa de desarrollo. Esto puede reforzar los intereses y vulnerabilidades existentes, al tiempo que reduce la diversidad de la exposición y crea bucles de retroalimentación de atención y refuerzo⁴⁵.

Al mismo tiempo, la formación de la identidad sigue siendo inestable. Esto hace que los niños de esta edad sean especialmente susceptibles a influencias externas, como las representaciones idealizadas y las normas basadas en la apariencia, sobre todo en los contextos visuales de los medios sociales y otros servicios digitales.

Riesgos para la salud mental

A medida que aumenta considerablemente la sensibilidad a la evaluación social, la autoestima y el bienestar emocional de los niños fluctúan. Esta etapa marca la aparición de riesgos interpersonales en línea, como el ciberacoso, la exclusión y las interacciones negativas entre iguales. Debido a la mayor sensibilidad a la evaluación social y la persistencia de la comunicación digital, estas experiencias pueden tener fuertes efectos emocionales.

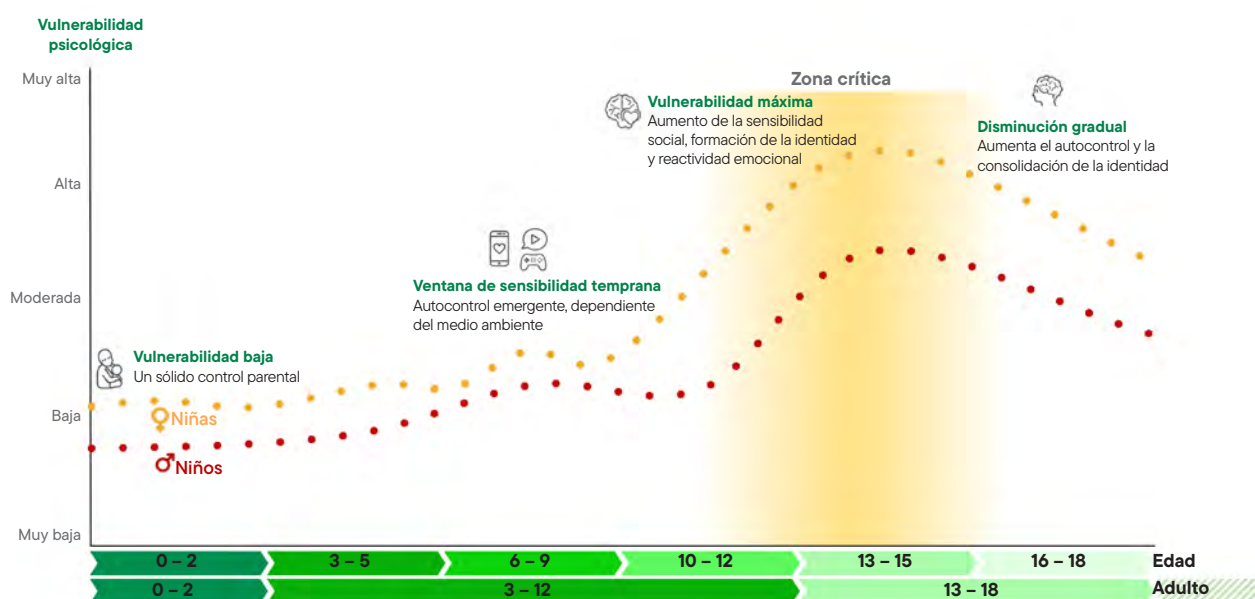
En cuanto al uso de teléfonos inteligentes, las investigaciones longitudinales prospectivas indican que, en el caso de los niños de 12 años, la adquisición de un teléfono inteligente puede estar relacionada con problemas de salud mental y falta de sueño a los 13 años. Por otra parte, las pruebas sugieren que la adquisición de un teléfono inteligente a los 13 años no está estadísticamente asociada con la depresión a los 14 años. Estos resultados también se ven influidos por la duración del uso. Esto sugiere que los niños de 13 años están más preparados emocionalmente para adquirir un teléfono inteligente, utilizar los medios sociales y otros servicios digitales y gestionar los posibles efectos negativos para su salud mental⁴⁶.

Para muchos niños, el período comprendido entre los 10 y los 12 años marca una etapa temprana en el desarrollo de problemas internalizantes, como la ansiedad y los síntomas depresivos. Estos problemas suelen verse influidos de forma bidireccional por el uso de los medios sociales y otros servicios digitales⁴⁷. Las dinámicas no se distribuyen de manera uniforme. Las pruebas indican que las niñas son especialmente vulnerables a la comparación basada en la apariencia y a la evaluación social mediada por las plataformas.

Las arquitecturas específicas de los medios sociales y otros servicios digitales también influyen en la exposición a los riesgos. En particular, la exposición a contenidos idealizados y centrados en la apariencia se ha asociado a la insatisfacción corporal y a una autopercepción negativa, sobre todo entre las niñas⁴⁸. A esta edad, las vulnerabilidades individuales, como el TDAH, la ansiedad o las dificultades sociales, interactúan con los entornos de los medios sociales y otros servicios digitales de formas más complejas, lo que a menudo refuerza los patrones de uso problemáticos⁴⁹. El impacto de los entornos de los medios sociales y otros servicios digitales en la salud mental y física de los niños, así como los factores de riesgo sociales e individuales, se analiza con más detalle en el capítulo 2.

Gráfico 4. Vulnerabilidad psicológica a lo largo del desarrollo

Sensibilidad a las dificultades de salud mental y a los riesgos digitales



CONCLUSIONES

Las edades comprendidas entre los 10 y los 12 años constituyen una etapa crítica en la que convergen la sensibilidad propia del desarrollo, la disminución de la supervisión y el uso de servicios digitales. Los riesgos digitales surgen de la interacción entre estos factores, más que del uso individual por sí solo. Por ello, esta etapa marca un punto de inflexión clave para la seguridad infantil en línea. El principal reto es la convergencia de la sensibilidad propia del desarrollo y los mecanismos de amplificación, que aumentan el riesgo de inestabilidad de la autoestima y de un uso problemático.

Esto requiere pasar de enfoques centrados en los progenitores a una regulación orientada a las estructuras y adaptada al desarrollo. El acceso a los dispositivos digitales en esta etapa debe regularse de forma cuidadosa. El uso debe producirse principalmente con el consentimiento y bajo la supervisión de los progenitores o en contextos educativos estructurados (por ejemplo, mediante aplicaciones de aprendizaje guiado en el ámbito escolar), en lugar de mediante la posesión personal de dispositivos sin restricciones. Este enfoque ayuda a equilibrar la participación temprana en el entorno digital con el establecimiento de los límites de protección necesarios.

Las respuestas institucionales, especialmente en las escuelas, deben fomentar las competencias y la alfabetización digitales, la resiliencia emocional y una participación crítica. La supervisión de los cuidadores sigue siendo esencial, sobre todo en el contexto del uso recreativo. Sin embargo, su eficacia se ve cada vez más limitada por la autonomía emergente de los niños y la complejidad de los medios sociales y otros servicios digitales.

RECOMENDACIONES (3-12 AÑOS)

Garantizar un uso supervisado de medios sociales y otros servicios digitales y dispositivos adecuados a la edad

A partir de los 3 años, las interacciones en línea de los niños deben limitarse, supervisarse y adaptarse gradualmente a la evolución de sus capacidades de manera estructurada. Debe evitarse el uso de dispositivos sin la autorización y la supervisión de los progenitores. Los cuidadores deben seguir dando prioridad a las interacciones cara a cara y a las actividades fuera de línea y garantizar que los niños duerman lo suficiente. En los entornos educativos, el uso que los niños y adolescentes hagan de los dispositivos proporcionados por la escuela debe tener una finalidad educativa definida. Las escuelas primarias deben estar, en gran medida, libres de dispositivos para proteger el desarrollo, las interacciones sociales y el aprendizaje de los niños.

Ofrecer a los niños y a sus círculos de apoyo una educación digital y de bienestar de calidad

Los niños y adolescentes deben tener acceso a una alfabetización digital y mediática de alta calidad (incluida la alfabetización en materia de IA) a lo largo de toda su escolarización, desde una edad temprana. Podría consultarse a los menores sobre el diseño de la alfabetización digital y mediática. La educación debe dotar a los niños y adolescentes de los conocimientos y las competencias que necesitan para comprender los riesgos y navegar de forma segura en línea.

Las competencias de autorregulación deben destacarse como una prioridad desde los primeros años de vida, no solo para los niños en edad escolar. Las escuelas deben garantizar que los niños y adolescentes reciban información sobre el bienestar y una educación de calidad en materia de salud mental. Deben ponerse a disposición recursos y profesionales pertinentes para apoyar a los niños, así como a los cuidadores y educadores (círculos de apoyo) en sus funciones de supervisión. Los círculos de apoyo deben ser capaces de reconocer los primeros indicios de negligencia digital, uso nocivo y abuso en línea y saber dónde pueden recibir apoyo.

13-18 años: la adolescencia como etapa de autonomía progresiva**13-15 AÑOS: LA PRIMERA ETAPA DE AUTONOMÍA PROGRESIVA**

La adolescencia entre los 13 y los 15 años constituye la etapa central de la formación de la identidad de los menores, caracterizada por una mayor exploración, inestabilidad y búsqueda de coherencia entre los distintos contextos sociales. Las relaciones entre iguales se convierten en el principal punto de referencia para la autoevaluación y el sentido de pertenencia. Las capacidades cognitivas se amplían, lo que permite un pensamiento abstracto más avanzado, una mayor capacidad para adoptar otras perspectivas y una mayor autorreflexión.

La toma de decisiones y la autorregulación también mejoran, pero siguen dependiendo del contexto, en particular en situaciones de fuerte carga emocional o social. El desarrollo de la identidad tiene lugar

cada vez más en entornos mediados digitalmente en los que la presentación de uno mismo, la valoración externa y la evaluación social son continuas, visibles y escalables⁵⁰.

Desde el punto de vista neurobiológico, la adolescencia se caracteriza por un desequilibrio entre unos sistemas emocionales y de recompensa muy activos y unos sistemas de control cognitivo aún en desarrollo. Mientras que los procesos límbicos^d aumentan la reactividad emocional y la sensibilidad a la valoración social, la corteza prefrontal (responsable del control de los impulsos y la autorregulación) madura de forma más gradual. Los cambios hormonales intensifican aún más la experiencia emocional.

Esto da lugar a una configuración del desarrollo en la que los adolescentes son más reactivos, más sensibles a la evaluación social y más propensos a asumir riesgos, especialmente en contextos de iguales. Aunque las capacidades de autorregulación mejoran, a menudo se ven superadas por la intensidad del procesamiento socioemocional⁵¹.

Desde el punto de vista psicológico, esta etapa se caracteriza por una intensificación del proceso de construcción de la identidad, una mayor variabilidad emocional y una creciente dependencia de la validación externa. La autoestima se vuelve inestable y depende de la valoración social, mientras que los adolescentes recurren cada vez más a una presentación intencional de sí mismos. Los entornos de los medios sociales y otros servicios digitales ofrecen posibilidades, como la capacidad de editar, la visibilidad y la una valoración cuantificable, que facilitan estos procesos⁵².

RETOS ESPECÍFICOS POR EDAD

Riesgos para la salud mental

Durante esta etapa, los medios sociales y otros servicios digitales se utilizan para regular las emociones y afrontar determinadas situaciones, lo que puede ofrecer beneficios a corto plazo, pero también puede reforzar la dependencia de la regulación externa⁵³. El uso de los medios sociales y otros servicios digitales por parte de los adolescentes como estrategia de regulación del estado de ánimo puede estar asociado a una mayor incidencia de depresión⁵⁴.

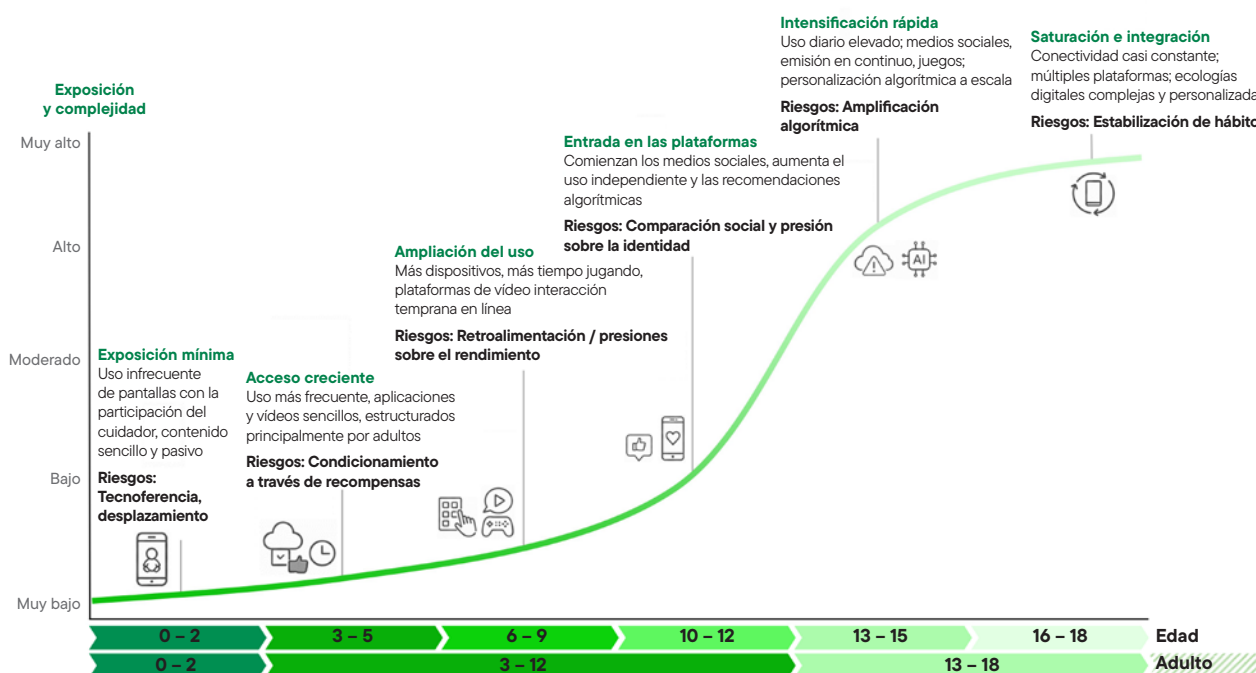
La adolescencia entre los 13 y los 15 años representa el momento de mayor vulnerabilidad a los problemas de salud mental, impulsada por la interacción de los cambios propios del desarrollo y las influencias ambientales. Esta etapa está asociada a un aumento de las tasas de trastornos internalizantes, como la depresión y la ansiedad⁵⁵. La mayor sensibilidad a la comparación social, la valoración externa y la exclusión crea vías específicas de vulnerabilidad en los entornos de los medios sociales y otros servicios digitales. Las presiones relacionadas con la presentación de sí mismos y la inestabilidad de la identidad pueden contribuir a una menor claridad del autoconcepto.

El comportamiento de asunción de riesgos alcanza su punto álgido y está fuertemente determinado por las dinámicas entre iguales. Esto puede verse amplificado por la visibilidad y la valoración externa en los entornos digitales. Los factores individuales y contextuales, como los problemas de salud mental preexistentes y el estrés familiar, interactúan con los entornos de los medios sociales y otros servicios digitales, lo que a menudo refuerza las vulnerabilidades con el paso del tiempo⁵⁶. Las pruebas longitudinales indican que estos riesgos no son uniformes. Se observan efectos negativos especialmente fuertes y persistentes entre las adolescentes.

d. El sistema límbico es un conjunto de estructuras cerebrales que intervienen en el procesamiento emocional, la motivación y la recompensa.

Gráfico 5. La exposición y la complejidad digitales a lo largo del desarrollo

El acceso, la intensidad y la complejidad de los entornos de los medios sociales+ aumentan



Riesgos relacionados con la IA, los medios sociales y otros servicios digitales

Los riesgos digitales en la adolescencia se ven intensificados por la convergencia del uso autónomo, la sensibilidad propia del desarrollo y los entornos estructurados algorítmicamente. Un riesgo de especial importancia específico de la IA en esta etapa tiene que ver con los agentes conversacionales y los denominados «asistentes de IA». Los adolescentes pueden utilizar estos sistemas no solo para el entretenimiento o la búsqueda de información, sino también para conversaciones personales, emocionales o relacionadas con situaciones de crisis.

Estas interacciones suelen estar diseñadas para ser afirmativas, poco conflictivas y disponibles de forma permanente. Si bien esto puede proporcionar una forma de apoyo de fácil acceso, también genera riesgos de apego unilateral y dependencia emocional. Esto puede ir acompañado de una menor exposición a la ambigüedad, el desacuerdo y la responsabilidad mutua que caracterizan a las relaciones humanas.

Cuando dichos sistemas son accesibles sin una verificación fiable de la edad ni salvaguardias adecuadas, surgen riesgos adicionales relacionados con la comunicación sexualizada, la manipulación, la captación sexual y los contenidos relacionados con situaciones de crisis. Los asistentes de IA no representan simplemente otra forma de contenido digital, sino un nuevo tipo de entorno socioemocional que requiere una atención específica en materia de desarrollo y regulación.

Un mecanismo central es la amplificación algorítmica. Los sistemas de recomendación dan prioridad a los contenidos que maximizan la interacción y suelen reforzar el material con una fuerte carga emocional y pertinente para la identidad. Esto puede configurar la percepción y el comportamiento con el tiempo al reforzar las vulnerabilidades existentes⁵⁷. Muchos medios sociales y otros servicios digitales promueven la evaluación social continua, exponiendo a los adolescentes a comentarios y comparaciones persistentes. Esto puede aumentar la volatilidad emocional y la dependencia de la validación externa.

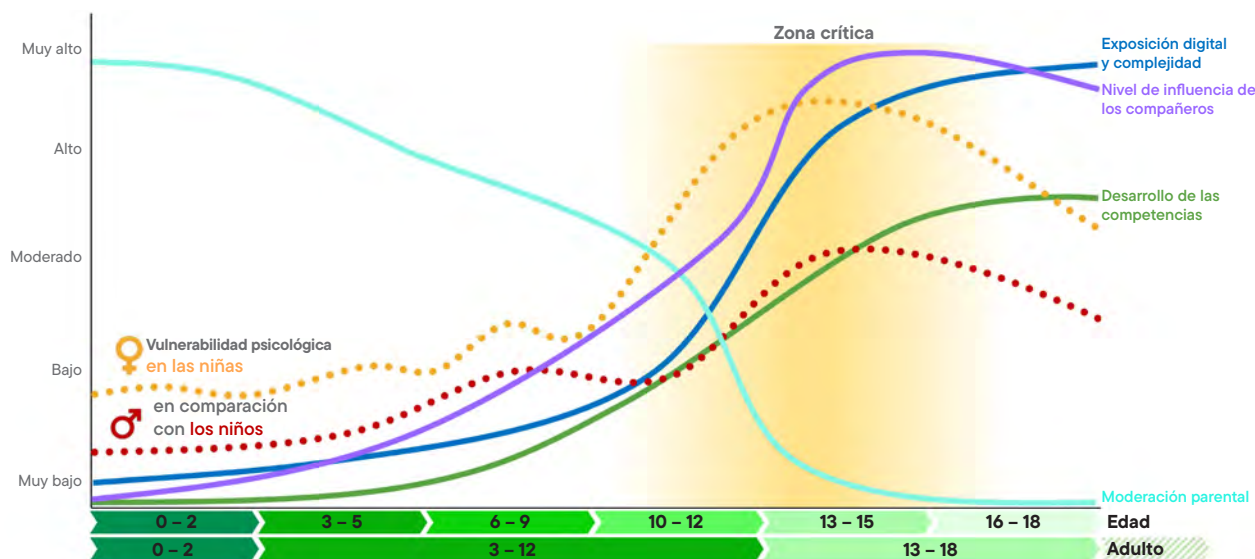
Riesgos de adicción

Determinadas características de diseño, como las recompensas variables, el desplazamiento infinito por la pantalla y la disponibilidad constante, contribuyen a un uso problemático o compulsivo e interactúan con la mayor sensibilidad de los adolescentes a las recompensas⁵⁸. El uso de los medios sociales y otros servicios digitales también se asocia con trastornos del sueño, una disminución del bienestar y sufrimiento emocional, aunque los efectos suelen ser reducidos y estar modulados por el contexto⁵⁹.

Es importante señalar que estos riesgos no son uniformes en todos los servicios ni tienen un carácter determinista. Surgen de la interacción entre las vulnerabilidades propias del desarrollo y las características digitales, lo que pone de relieve la necesidad de ir más allá de los modelos simplificados sobre el impacto de los servicios digitales⁶⁰.

Gráfico 6. Un desajuste en el desarrollo entre la exposición digital, la vulnerabilidad y la capacidad de regulación

Las trayectorias combinadas ponen de manifiesto que la exposición digital aumenta rápidamente, mientras que la mediación parental disminuye y las competencias de regulación se desarrollan a un ritmo más lento. Esta tendencia coincide con un pico de vulnerabilidad psicológica durante la adolescencia.



CONCLUSIONES

A partir de los 13 años, los adolescentes pasan de un uso supervisado de los servicios en línea a un uso guiado. Los adolescentes tienen más libertad para explorar las oportunidades que ofrece el mundo en línea para relacionarse, aprender y desarrollar su creatividad. Los medios sociales y otros servicios digitales les ofrecen la oportunidad de desarrollar sus pasiones e intereses y compartirlos con los demás.

La transición a la autonomía es una parte normal del crecimiento en el mundo actual de internet, al igual que en el mundo real. La cuestión no es cómo frenar esta transición de los adolescentes, sino limitar su exposición a posibles peligros durante una etapa de su desarrollo en la que la vulnerabilidad es máxima. Esta vulnerabilidad se caracteriza por la convergencia de la formación de la identidad, una mayor sensibilidad socioemocional y entornos estructurados algorítmicamente.

Los riesgos digitales no se derivan de la exposición por sí sola, sino de su intensidad y de la estructura de los medios sociales y otros servicios digitales, diseñados para maximizar la interacción en una etapa de mayor vulnerabilidad. Estos factores hacen de la adolescencia una etapa fundamental tanto para la investigación como para la regulación.

A esta edad, las formas tradicionales de supervisión por parte de cuidadores y educadores resultan cada vez más ineficaces y difíciles de aplicar. Los riesgos proceden cada vez más de las estructuras de los medios sociales y otros servicios digitales, más que del comportamiento individual por sí solo. Un reto clave reside en abordar los sistemas algorítmicos que estructuran la exposición e influyen en el comportamiento y funcionan con una transparencia limitada.

Los enfoques reguladores deben equilibrar la protección con la necesidad de autonomía y participación en línea de los adolescentes. Una protección eficaz requiere un enfoque multinivel diferenciado por etapas del desarrollo que combine la regulación de los medios sociales+, las intervenciones educativas y el apoyo a la autorregulación y al uso crítico de los servicios digitales.

Las investigaciones recientes indican que las prohibiciones generales de uso de los medios sociales y otros servicios digitales pueden ser menos eficaces de lo que a menudo se supone. Si bien estas medidas tienen por objeto reducir la exposición y los riesgos conexos, las pruebas de su eficacia son actualmente limitadas, en particular en el caso de los adolescentes. Los enfoques excesivamente restrictivos pueden eludirse o desplazar los riesgos hacia entornos menos regulados.

En este contexto, se ha propuesto un modelo de participación regulada por franjas de edad, que combina la verificación de la edad con protección de la privacidad, la seguridad desde el diseño y la educación mediática, como alternativa más sensible a las distintas etapas del desarrollo. Este enfoque adapta las medidas de protección a la evolución de las capacidades de los niños, equilibrando la seguridad, la participación y los derechos de los niños en un marco integrado para la seguridad infantil en línea.

16-18 AÑOS: LA SEGUNDA ETAPA DE AUTONOMÍA PROGRESIVA

La adolescencia tardía marca una etapa de creciente consolidación de la identidad y de mayor autonomía. Los roles, valores y autoconceptos previamente explorados empiezan a estabilizarse, dando lugar a representaciones de uno mismo más coherentes e internamente integradas. Mientras tanto, las capacidades cognitivas alcanzan un mayor nivel de sofisticación. Esto incluye el razonamiento abstracto, la planificación a largo plazo y la toma de decisiones reflexiva.

Estos avances favorecen una participación más autónoma en los sistemas sociales, educativos y económicos. Los medios sociales y otros servicios digitales ya no son espacios de exploración, sino que están plenamente integrados en la vida cotidiana y configuran la comunicación, la participación y la autoexpresión⁶¹. Desde el punto de vista neurobiológico, el cerebro se aproxima a la madurez funcional, especialmente en la corteza prefrontal. Esto da lugar a una mejora del autocontrol, la planificación y la toma de decisiones.

Los sistemas emocionales y cognitivos están más integrados, lo que permite una regulación emocional más estable y una mejor anticipación de las consecuencias a largo plazo. Sin embargo, el desarrollo aún no ha concluido, ya que la maduración continúa hasta principios de la edad adulta⁶². Esto da lugar a un perfil de mayor estabilidad, combinada con una sensibilidad continuada ante entornos muy estimulantes.

RETOS ESPECÍFICOS POR EDAD

Dependencia de la trayectoria

A pesar de la creciente madurez durante esta etapa, siguen existiendo vulnerabilidades. Los problemas de salud mental surgidos en etapas anteriores pueden persistir, especialmente cuando no se han abordado los mecanismos subyacentes⁶³. Esto pone de relieve la necesidad de proteger a los menores frente a posibles daños, no solo durante la adolescencia, sino desde las edades más tempranas.

La autorregulación, aunque ha mejorado, sigue dependiendo del contexto y puede verse comprometida por entornos digitales muy absorbentes. Además, la consolidación de los patrones de comportamiento introduce una dependencia de la trayectoria, lo que hace que los hábitos ya establecidos sean más resistentes al cambio. Los riesgos digitales a esta edad están menos relacionados con su aparición que con su estabilización y refuerzo.

Riesgos de uso problemático

Los patrones de uso ya establecidos, incluido el uso problemático y excesivo o la adicción, se mantienen y refuerzan mediante determinadas características de los medios sociales y otros servicios digitales (por ejemplo, las recomendaciones personalizadas, los flujos continuos de contenido y la interacción basada en recompensas)⁶⁴. Los sistemas algorítmicos siguen configurando la exposición y el comportamiento, a menudo de forma subconsciente⁶⁵. Por último, las vulnerabilidades siguen estando determinadas por desigualdades estructurales, como el entorno familiar y el acceso a los recursos⁶⁶.

El uso de los medios sociales y otros servicios digitales sigue estando asociado a determinados resultados, como los trastornos del sueño, el estrés emocional y la comparación social. Sin embargo, los efectos se deben cada vez más a patrones de uso a largo plazo, más que a una sensibilidad aguda propia del desarrollo⁶⁷. Los riesgos relacionados con la explotación de datos, la influencia comercial y la participación en las economías digitales cobran mayor importancia a medida que los adolescentes participan más activamente en los medios sociales y otros servicios digitales.

CONCLUSIONES

La adolescencia tardía supone un reto para la seguridad infantil en línea, ya que marca la transición de la minoría de edad protegida a la mayoría de edad. El principal reto a esta edad es conciliar la creciente autonomía de los adolescentes con las vulnerabilidades persistentes propias del desarrollo.

Otra cuestión importante es la aparición de una discrepancia. Las personas de entre 16 y 18 años suelen ser tratadas como usuarios plenamente autónomos, a pesar de que sus procesos de desarrollo aún están en curso. Esto pone de relieve la necesidad de adoptar enfoques reguladores que vayan más allá de los umbrales de edad rígidos y tengan en cuenta las transiciones graduales propias del desarrollo.

Una protección eficaz en esta etapa no solo debe abordar el acceso y los contenidos, sino también las condiciones estructurales que determinan el comportamiento a largo plazo, incluido el diseño de los medios sociales y otros servicios digitales, los sistemas algorítmicos y las prácticas relacionadas con los datos. Durante esta etapa de creciente autonomía, se debe apoyar a los adolescentes para que desarrollen prácticas sostenibles y reflexivas en relación con el uso de los medios sociales y otros servicios digitales, incluida la autorregulación y una conciencia crítica de los entornos digitales.

Los riesgos son cada vez más acumulativos y vienen determinados por los hábitos ya establecidos y las influencias estructurales, más que por la sensibilidad inmediata propia de esta etapa de desarrollo. Por lo tanto, la seguridad infantil en línea debe extenderse a esta etapa para abordar la transición hacia una participación autónoma, teniendo en cuenta, al mismo tiempo, la persistencia de determinadas vulnerabilidades propias del desarrollo. Las medidas deben promover el desarrollo de prácticas sostenibles de participación que guíen a los adolescentes en su transición hacia la edad adulta.

RECOMENDACIONES (13-18 AÑOS)

Garantizar un uso cada vez más autónomo de medios sociales y otros servicios digitales adecuados a la edad

A partir de los 13 años, los adolescentes pueden comenzar una transición de un uso supervisado de los medios sociales y otros servicios digitales a un uso autónomo. Los progenitores, cuidadores, profesores y educadores siguen desempeñando un papel importante a la hora de orientar las interacciones en línea de los adolescentes. Los círculos de apoyo de los adolescentes deben seguir fomentando las interacciones cara a cara y las actividades fuera de línea, incluido un sueño suficiente. En los entornos educativos, el uso de dispositivos debe tener una finalidad educativa definida.

Conclusión

En este capítulo se han analizado las características definitorias y los riesgos asociados al uso de los servicios en línea por parte de los niños en tres etapas principales de su desarrollo: la primera infancia (0-2 años), la infancia (3-12 años) y la adolescencia (13-18 años). Se han presentado recomendaciones generales para orientar a los proveedores de medios sociales y otros servicios digitales, los reguladores, los cuidadores y los educadores en la aplicación de un enfoque de la seguridad infantil en línea adaptado a la edad, de conformidad con sus respectivas competencias y responsabilidades.

Sobre la base de un análisis de las pruebas disponibles sobre los riesgos para la salud y el bienestar de los menores a lo largo de estas etapas de desarrollo, se ha esbozado un enfoque por etapas para orientar las interacciones en línea de niños y adolescentes en tres etapas principales:

- // 0-2 años: la primera infancia como etapa de desarrollo especialmente protegida;
- // 3-12 años: la infancia como etapa de desarrollo supervisada;
- // 13-18 años: la adolescencia como etapa de autonomía progresiva.

En el capítulo 3 se analizan con más detalle los marcos e instrumentos existentes en materia de protección infantil en línea. En el capítulo 4 se presentan medidas destinadas a empoderar a los menores en línea y a sus círculos de apoyo para orientar el uso que hacen los niños y adolescentes de los medios sociales y otros servicios digitales. En el siguiente capítulo se examinan con más detalle los riesgos a los que se enfrentan los niños en línea en las diferentes etapas de su desarrollo, también en relación con diversos factores sociales e individuales.

02

Pruebas sobre los riesgos a los que se enfrentan los menores en línea

Como se ha mencionado en el capítulo 1, la seguridad infantil en línea no puede conceptualizarse únicamente desde una perspectiva del desarrollo. Factores como el contexto socioeconómico y el género ejercen una influencia importante en los patrones de uso de servicios en línea por parte de niños y adolescentes, así como en su susceptibilidad a los riesgos conexos⁶⁸. La sexualidad, el origen racial y étnico, la religión, el origen migrante y las necesidades educativas especiales también influyen en la exposición de los menores a posibles daños.

En el presente capítulo se analiza el segundo de los seis principios rectores propuestos por los copresidentes como marco para orientar la acción: la igualdad y la diversidad. Se describe la manera en que las desigualdades en cuanto a los riesgos y la exposición a posibles daños en línea entre diferentes grupos de edad y grupos socioeconómicos se entrecruzan con las necesidades de los menores a lo largo de su desarrollo. Asimismo, se evalúa la exposición de los menores a diversos riesgos en línea (por ejemplo, contenidos ilícitos y características de diseño perjudiciales de los medios sociales y otros servicios digitales) que repercuten en su salud física y mental.

En la actualidad, **existen muchas más pruebas (por ejemplo, centradas en el ciberacoso y los contenidos nocivos) de una posible asociación negativa entre el uso de los medios sociales y la salud mental** que de sus efectos positivos. Gran parte de las pruebas relativas al potencial de los medios sociales para perjudicar la salud y el bienestar de los menores son de carácter correlacional, por lo que no permiten extraer conclusiones causales. No obstante, ofrecen indicios suficientes para justificar la adopción de medidas destinadas a proteger a los menores en línea.

A pesar de la disponibilidad de pruebas en determinados ámbitos, algunas lagunas de datos dificultan un análisis exhaustivo que permita incorporar los factores de riesgo sociales e individuales desde una perspectiva del desarrollo. En términos más generales, la falta de transparencia y de acceso a los datos de los medios sociales dificulta la investigación sobre los efectos positivos y negativos del uso de los medios sociales por parte de los menores⁶⁹.

Un mayor número de estudios longitudinales y de conjuntos de datos a escala europea podría ayudar a comprender mejor y con mayor detalle las consecuencias de los riesgos a los que se enfrentan los niños

y adolescentes en los distintos medios sociales y otros servicios digitales. Cualquier examen detallado sobre los menores requiere especial cuidado desde el punto de vista de la ética de la investigación⁷⁰.

Algunas de las pruebas recopiladas también han dado lugar a algunas ideas erróneas en el debate público. Un ejemplo son las afirmaciones sobre la supuesta «podredumbre cerebral» causada por los medios sociales, con algunos informes que sugieren que un uso excesivo de estos medios podría reducir la materia gris del cerebro humano⁷¹. Tales afirmaciones son excesivamente reduccionistas y no se basan en pruebas médicas.

El presente capítulo tiene por objeto presentar y reforzar la base empírica actual. Es fundamental disponer de pruebas sólidas sobre cómo los riesgos y los daños se relacionan con los distintos servicios digitales, y no solo los medios sociales, para fundamentar las medidas adecuadas para proteger y empoderar a los menores en línea. En el capítulo 4 se analizan las oportunidades que ofrece el mundo digital a los niños y adolescentes.

Factores de riesgo sociales e individuales

GÉNERO Y SEXUALIDAD

Riesgos para las niñas y los niños

Las niñas y las jóvenes están especialmente expuestas a una serie de daños específicos relacionados con el género en línea. Entre ellos figuran el acoso de carácter sexista y misógino y una exposición desproporcionada a daños de naturaleza sexual⁷², como la difusión no consentida de imágenes íntimas y ultrafalsificaciones sexualmente explícitas en línea⁷³.

En términos más generales, las investigaciones sugieren que las niñas tienen más probabilidades de sufrir ciberacoso que los niños⁷⁴. Un estudio reveló que hasta el 63 % de las niñas en Europa han declarado haber sufrido algún tipo de acoso en línea en los medios sociales⁷⁵.

Existen algunas pruebas de que **los daños a los que se ven expuestas las jóvenes y las niñas en línea evolucionan con la edad**. Las niñas de entre 13 y 15 años pueden tener más probabilidades de sufrir exclusión de chats grupales, comentarios despectivos sobre su cuerpo, chismes y humillación pública⁷⁶. Por su parte, las niñas y jóvenes de entre 11 y 18 años pueden estar más expuestas a formas de abuso de carácter sexual o controlador, como la coacción, las ultrafalsificaciones y la captación sexual. Si bien las niñas de esta edad están especialmente expuestas a estos riesgos, los niños también lo están.

La creciente omnipresencia de la inteligencia artificial (IA) y su integración en aplicaciones y servicios en línea aumenta los riesgos⁷⁷. Por ejemplo, las ultrafalsificaciones pueden utilizarse con fines maliciosos para ciberacosar a otras personas⁷⁸. Desde su aparición, la creación de ultrafalsificaciones ha ido en aumento y puede utilizarse para cometer abusos sexuales en línea⁷⁹. Las ultrafalsificaciones han introducido una nueva dimensión de daño que no solo perjudica la reputación de una persona, sino que, al igual que otros actos de ciberacoso, también puede provocar un trauma psicológico.

Las niñas pueden estar más expuestas a daños relacionados con la comparación social en línea y tener más probabilidades de desarrollar una imagen negativa de su propio cuerpo⁸⁰. Las investigaciones indican que la presión entre iguales en relación con los ideales de imagen corporal puede verse agravada por el uso de servicios en línea⁸¹.

Por ello, las niñas pueden tener más probabilidades de unirse a comunidades en línea que fomentan los trastornos alimentarios, o de promover dichas comunidades⁸². Las pruebas indican una relación entre las interacciones en línea de las adolescentes relacionadas con la presentación de sí mismas, incluido el uso de los medios sociales, y los efectos negativos para la salud mental, como la depresión y la ansiedad⁸³. Las niñas de entre 10 y 12 años pueden estar especialmente expuestas a estos riesgos.

Como pauta general, las niñas pasan más tiempo en los medios sociales y utilizan con mayor frecuencia las funciones de chat en línea que los niños⁸⁴. Algunos estudios han asociado un uso moderado o intensivo de los servicios digitales entre las niñas con una mayor prevalencia de problemas de salud mental y un menor bienestar⁸⁵.

Los niños, por su parte, son más propensos a dedicar tiempo a los videojuegos en línea. Varios estudios han demostrado que el uso de videojuegos en línea está asociado a problemas de salud mental, como la depresión y la ansiedad. Sin embargo, la asociación entre el uso de los medios sociales y los problemas de salud mental puede ser más fuerte que la observada en relación con los videojuegos⁸⁶. El riesgo de transgresiones sexuales en línea es mayor para los niños en comparación con entornos del mundo real. A menudo se subestima su vulnerabilidad en estos entornos⁸⁷.

Por último, las niñas y los niños pueden afrontar los daños en línea de maneras diferentes. En el caso del ciberacoso, es posible que los jóvenes varones sean más propensos a utilizar técnicas de afrontamiento evasivas, debido a normas que los animan a gestionar sus problemas por sí mismos, en lugar de buscar ayuda en sus círculos de apoyo⁸⁸. Tanto en niñas como en niños, los estudios relacionan un mayor uso de los medios sociales con una peor salud mental y un menor bienestar⁸⁹.

Comunidades LGBTIQ+

Los niños y adolescentes con orientaciones sexuales diversas tienen más probabilidades de experimentar odio⁹⁰ y violencia en línea, incluido el ciberacoso⁹¹ y el acoso sexual⁹². Los servicios digitales también pueden agravar las experiencias de los jóvenes usuarios LGBTIQ+ relacionadas con la captación sexual, las agresiones sexuales y el riesgo de que se revele su orientación sexual sin su consentimiento⁹³.

A nivel de población, entre las personas pertenecientes a las comunidades LGBTIQ+, el 63 % declara haberse encontrado con contenidos violentos en línea y desinformación dirigidos contra estas comunidades⁹⁴. Las pruebas sugieren que los adolescentes pertenecientes a las comunidades LGBTIQ+ pueden ser más propensos a utilizar espacios en línea para explorar su sexualidad e identidad, buscar información sobre salud sexual o buscar apoyo y conexión entre iguales sin exponerse a los riesgos «presenciales»⁹⁵.

Esto puede aumentar la exposición de los niños y adolescentes LGBTIQ+ a riesgos y daños en línea. A pesar de los numerosos argumentos a favor del potencial de los espacios en línea para ofrecer a los niños y adolescentes con orientaciones sexuales diversas la oportunidad de conectarse y recibir apoyo entre iguales, las pruebas sugieren que las interacciones presenciales pueden seguir siendo más eficaces a la hora de ofrecer apoyo que las interacciones en línea⁹⁶.

CONTEXTO SOCIOECONÓMICO

Los adolescentes procedentes de contextos socioeconómicos desfavorecidos tienen más probabilidades de tener experiencias negativas en línea, como el ciberacoso⁹⁷, el uso excesivo de dispositivos, la adicción a los medios sociales⁹⁸ y su uso problemático⁹⁹. Los factores socioeconómicos, como unos ingresos fa-

miliars más bajos, también pueden aumentar la prevalencia de experiencias perjudiciales en línea entre los niños y adolescentes¹⁰⁰.

El contexto familiar ejerce una influencia importante en la exposición de los menores a posibles daños en línea. Los niños y adolescentes cuyos progenitores presentan un bajo nivel de alfabetización digital pueden estar más expuestos a daños en línea¹⁰¹. Las pruebas sugieren que los menores procedentes de contextos socioeconómicos menos favorecidos tienden a presentar niveles más bajos de alfabetización digital, lo que puede dificultar una navegación segura en línea, y pueden adoptar comportamientos más arriesgados en estos entornos¹⁰².

Por otra parte, las familias más privilegiadas pueden estar mejor preparadas y disponer de más recursos para orientar de forma positiva la interacción de sus niños y adolescentes con las tecnologías digitales¹⁰³ y abordar los efectos negativos. De este modo, el uso problemático de los servicios digitales, incluidos los medios sociales, puede reforzar las desigualdades existentes en materia de salud, participación académica y rendimiento entre los adolescentes y adultos jóvenes.

Si bien el hecho de vivir en una zona urbana o rural puede no influir directamente en la exposición de los menores a daños en línea, los niños y adolescentes que viven en zonas rurales pueden ser más propensos a recurrir a mecanismos de afrontamiento evasivos, que están más estrechamente asociados a resultados negativos en materia de salud mental. Esto pone de relieve la necesidad de desarrollar programas que aborden las desigualdades sociales, también en las zonas rurales e insuficientemente atendidas, con el fin de reducir la probabilidad de que los menores sufran daños en línea¹⁰⁴.

ORIGEN RACIAL Y ÉTNICO, RELIGIÓN Y ORIGEN MIGRANTE

Los adolescentes pertenecientes a minorías raciales tienen más probabilidades de sufrir daños en línea, como ciberacoso, discriminación racial y acoso¹⁰⁵. Las pruebas procedentes de Europa indican que el discurso de odio en línea se dirige con frecuencia contra personas por razón de su origen racial o étnico, religión, nacionalidad u origen migrante, siendo las personas negras, romaníes, judías y musulmanas algunos de los grupos más frecuentemente afectados¹⁰⁶. Además, el racismo, el odio por motivos religiosos, el odio por razón de orientación sexual y el sexismo son algunas de las formas de discurso de odio más frecuentes en línea¹⁰⁷.

Las pruebas procedentes de la Unión Europea sugieren, además, que estas experiencias en línea reflejan patrones más amplios de discriminación que afectan a las comunidades minoritarias. Según la Agencia de los Derechos Fundamentales de la Unión Europea (FRA), casi la mitad (47 %) de los musulmanes encuestados en trece Estados miembros de la UE declararon haber sufrido discriminación racial durante los cinco años anteriores. Esto incluye el acoso y la discriminación en la educación, el empleo y los espacios públicos. Muchos también declararon haber estado expuestos a manifestaciones de hostilidad antimusulmana en línea¹⁰⁸. Del mismo modo, la encuesta de la FRA a personas de ascendencia africana reveló que casi la mitad de los encuestados había sufrido discriminación racial y los entornos en línea se señalaron como un contexto importante en el que se producen abusos racistas¹⁰⁹.

Parece haber una creciente normalización y trivialización del discurso de odio en línea. La Comisión Europea contra el Racismo y la Intolerancia (ECRI) del Consejo de Europa ha puesto de relieve los crecientes niveles de discurso de odio en toda Europa. Señala que el origen étnico y la religión se encuentran entre los factores de riesgo más frecuentes asociados al discurso de odio en línea y advierte de que la retórica xenófoba, antimusulmana, antisemita y antinegra se ha normalizado cada vez más en los espacios digitales¹¹⁰.

Además, a nivel de población, las pruebas sugieren que las personas pertenecientes a minorías pueden verse afectadas de manera desproporcionada por las restricciones y las medidas de eliminación aplicadas por los sistemas de moderación de contenidos, como consecuencia de los sesgos en los algoritmos utilizados en dichos sistemas¹¹¹. Esto refleja preocupaciones más amplias en relación con los sesgos étnicos y de género presentes en los modelos de detección y predicción del lenguaje utilizados por los proveedores de servicios digitales para analizar automáticamente los contenidos nocivos en línea¹¹².

NIÑOS CON NECESIDADES EDUCATIVAS ESPECIALES

Las pruebas indican que los jóvenes con necesidades educativas especiales y con discapacidad tienen más probabilidades de sufrir daños¹¹³, como el discurso de odio, el ciberacoso, las ciberamenazas, el acoso, la exposición a contenidos sexuales y la captación sexual en línea¹¹⁴.

Factores como las barreras de comunicación y la alfabetización emocional pueden exacerbar las vulnerabilidades existentes de los niños y adolescentes con discapacidad en los espacios en línea¹¹⁵. El aislamiento social y la sensación de vulnerabilidad que experimentan los menores con discapacidad aumentan considerablemente el riesgo de victimización¹¹⁶.

Las pruebas sugieren que los niños y adolescentes con discapacidad pueden sentirse más cómodos a la hora de expresarse en los espacios en línea¹¹⁷. Además, los menores con discapacidad utilizan los entornos en línea en mayor medida para compartir sus intereses y aficiones, jugar con otras personas y buscar información sanitaria y apoyo emocional, a pesar de estar más expuestos a posibles daños en línea¹¹⁸.

Del mismo modo, las investigaciones sugieren que los niños y adolescentes con trastornos del neurodesarrollo, incluido el trastorno de déficit de atención e hiperactividad (TDAH), están más expuestos a un uso problemático de los entornos en línea¹¹⁹. Además, los menores con características del trastorno del espectro autista y con trastornos intelectuales y del desarrollo presentan una probabilidad cada vez mayor de ser objeto de acoso en línea¹²⁰. Un tiempo prolongado frente a las pantallas también puede estar asociado a un aumento de los síntomas del TDAH¹²¹.

Es importante señalar que los factores de riesgo sociales e individuales que afectan a los niños y adolescentes en línea se entrecruzan. Por ejemplo, los menores con discapacidad pueden tener más probabilidades de experimentar discursos de odio en línea dirigidos contra su género, sexualidad, raza o religión¹²². Esto demuestra la necesidad de tener en cuenta la interacción entre diversos factores sociales e individuales y la manera en que estos agravan la exposición de determinados grupos sociales a posibles daños a la hora de diseñar medidas destinadas a promover la seguridad infantil en línea.

RIESGOS PARA LA SALUD MENTAL

Según datos de la Organización Mundial de la Salud, uno de cada siete jóvenes de entre 10 y 19 años en todo el mundo padece algún problema de salud mental¹²³. A escala europea, la encuesta del Eurobarómetro de 2023 sobre salud mental puso de manifiesto que el 59 % de los jóvenes había experimentado un problema emocional o psicosocial, como sentirse deprimido o ansioso¹²⁴.

Entre los adolescentes, la depresión, la ansiedad y los trastornos del comportamiento se encuentran entre las principales causas de enfermedad¹²⁵. A escala mundial, el suicidio es una de las principales causas de muerte entre los jóvenes¹²⁶ (véase más adelante: «Autolesiones deliberadas y conducta suicida»). A nivel de población, los grupos vulnerables, incluidas las personas pertenecientes a las comunidades LGBTQ+, las de origen migrante y las refugiadas, son los que corren mayor riesgo¹²⁷.

Las pruebas indican que las niñas son especialmente vulnerables, por ejemplo, a la comparación basada en la apariencia y a la evaluación social mediada por las plataformas. Para muchos menores, las edades comprendidas entre los 10 y los 12 años marcan una etapa temprana en el desarrollo de problemas internalizantes, como la ansiedad y los síntomas depresivos. Los problemas de salud mental pueden continuar en la adolescencia, que representa el punto álgido de vulnerabilidad, si no se abordan los mecanismos subyacentes.

Los problemas de salud mental no solo tienen graves consecuencias directas para el bienestar y el desarrollo de niños y adolescentes, sino que también repercuten en la asistencia y el rendimiento escolar de los menores y, más adelante, en su empleabilidad¹²⁸. Los datos sugieren que el uso de los servicios digitales, en particular de los medios sociales, tiene amplios efectos en la salud y el desarrollo de los niños y adolescentes.

Un estudio indicó que un uso excesivo de los medios sociales de más de tres horas al día puede estar asociado a consecuencias negativas para la salud mental, especialmente depresión y ansiedad¹²⁹. Del mismo modo, los resultados de la evaluación PISA de 2022, que abarcó a veintidós Estados miembros de la UE, mostraron que la probabilidad estimada de que los jóvenes de 15 años sufran problemas de salud mental aumenta con el tiempo que pasan en línea¹³⁰.

PRUEBAS DE UNA RELACIÓN BIDIRECCIONAL ENTRE LOS PROBLEMAS DE SALUD MENTAL Y EL USO DE LOS SERVICIOS DIGITALES

La relación entre la interacción de los niños y adolescentes con el mundo de los medios sociales y otros servicios digitales y los problemas de salud mental es compleja. En lo que respecta a los medios sociales, las pruebas apuntan a una relación bidireccional entre las interacciones en línea de los menores y la prevalencia de problemas de salud mental¹³¹. Esto significa que las interacciones de los niños y adolescentes con los espacios en línea pueden causar problemas de salud mental, pero también reforzar los ya existentes, en particular, la depresión¹³².

Las pruebas disponibles respaldan la idea de que las experiencias negativas en línea son muy frecuentes entre los adolescentes que ya padecen problemas de salud mental¹³³. Los adolescentes que experimentan ansiedad social pueden ser especialmente propensos a pasar más tiempo en los medios sociales o a desarrollar patrones de uso problemático¹³⁴. Las personas con ansiedad social a veces recurren a los medios sociales para entablar relaciones positivas en línea y aliviar la ansiedad que les provocan las interacciones presenciales, pero esto puede fomentar comportamientos evasivos.

«Hay que adoptar una visión más amplia y detallada de las distintas tecnologías implicadas. [...] Centrarse únicamente en los medios sociales es demasiado limitado, ya que otras tecnologías, como la IA generativa, plantean riesgos comparables, si no mayores, para los menores.»

— JUDITH SIMON,
PROFESORA DE ÉTICA DE LAS
TECNOLOGÍAS DE LA INFORMACIÓN,
UNIVERSIDAD DE HAMBURGO

Del mismo modo, es probable que la exposición de los menores a contenidos inadecuados para su edad, incluidos aquellos que muestran o fomentan las autolesiones físicas, los trastornos alimentarios y el suicidio, agrave los trastornos preexistentes.

En el caso de los adolescentes que utilizan los medios sociales, la calidad de sus redes fuera de línea y ciertos rasgos de personalidad, como la introversión o la extroversión, pueden actuar como factores de protección o de riesgo. Las investigaciones sugieren que el uso de los medios sociales por parte de adolescentes extrovertidos con buena autoestima y amistades de alta calidad fuera de línea puede reforzar sus relaciones presenciales y aumentar el apoyo en línea.

Por otra parte, los adolescentes introvertidos con baja autoestima y redes sociales más débiles fuera de línea pueden ser más propensos a buscar nuevas amistades en línea. Esto puede aumentar los posibles riesgos de exposición a contactos o contenidos no deseados¹³⁵.

HERRAMIENTAS Y ASISTENTES DE IA EN LOS MEDIOS SOCIALES Y OTROS SERVICIOS DIGITALES

Los recientes avances tecnológicos han acelerado el uso de la IA generativa, los chatbots basados en grandes modelos de lenguaje y los «asistentes de IA» por parte de niños y adolescentes. Este cambio ha ido acompañado de una creciente preocupación por las repercusiones de estas tecnologías para la salud mental y el bienestar de los menores. Esta es la razón por la que los copresidentes han optado por el término amplio «medios sociales y otros servicios digitales» en el presente informe.

A diferencia de las herramientas digitales de salud mental anteriores, incluidas las aplicaciones y la realidad virtual, que tuvieron dificultades para mantener su uso, millones de niños y adolescentes ya utilizan chatbots de IA para buscar información (también sobre cuestiones de salud mental), interactuar y obtener apoyo emocional. Algunas pruebas preliminares sugieren posibles beneficios, como el potencial de los agentes conversacionales de IA para ayudar a reducir los síntomas de la depresión¹³⁶.

Las investigaciones también indican posibles beneficios de las interfaces basadas en IA para favorecer una educación inclusiva entre los alumnos con discapacidades visuales, físicas y cognitivas¹³⁷. Sin embargo, el impacto de las herramientas de IA en la educación y el desarrollo de competencias de los menores debe analizarse más a fondo para comprender los posibles beneficios y riesgos¹³⁸.

Están surgiendo señales preocupantes tanto en los medios de comunicación como en las primeras investigaciones sobre la posible aparición, asociada a la IA, de síntomas «psicóticos», apego parasocial, patrones de dependencia¹³⁹ e incitación al suicidio¹⁴⁰. Las pruebas sugieren que los menores a menudo perciben a los «asistentes de IA» como si fueran seres humanos¹⁴¹. Sin embargo, es posible que no proporcionen un apoyo empático genuino y pueden plantear riesgos para la salud mental de los menores¹⁴².

Los niños de corta edad pueden ser especialmente susceptibles de crear vínculos emocionales con los asistentes de IA, a los que pueden percibir como interlocutores sociales con capacidad de respuesta. Los adolescentes que utilizan estas herramientas para intercambios personales y emocionales también están expuestos a riesgos de apego y dependencia.

Un estudio europeo reciente demostró que más del 86 % de los adolescentes irlandeses, franceses, alemanes y suecos utilizan herramientas de IA. Entre ellos, más de la mitad utiliza estas herramientas para hablar de temas íntimos y resolver problemas personales¹⁴³. Este estudio indicó que los adolescentes que utilizan herramientas de IA son más propensos a sufrir síntomas de ansiedad.

Los sistemas de IA pueden explotar las vulnerabilidades de los menores al abusar de su curiosidad natural, su deseo de recompensas, su susceptibilidad a la presión y su tendencia a buscar una gratificación inmediata. También pueden exacerbar el impacto de técnicas de diseño manipuladoras, como el «nudging» conductual¹⁴⁴.

Los sesgos algorítmicos y sociales incorporados en los datos de entrenamiento de la IA también pueden favorecer la difusión de desinformación, información errónea y estereotipos que los menores pueden interiorizar desde una edad temprana¹⁴⁵. Las consecuencias de la explotación facilitada por la IA pueden ser graves y duraderas para los niños y adolescentes, incluidas conductas adictivas, una reducción de la capacidad de concentración y de las capacidades cognitivas, un bajo rendimiento académico y dificultades sociales.

Los niños de entre 6 y 12 años pueden estar especialmente expuestos al desarrollo temprano de conductas adictivas, que pueden continuar hasta los primeros años de la adolescencia y más allá. Se necesitan más investigaciones, no solo sobre las oportunidades que las herramientas de IA ofrecen a los niños y adolescentes, sino también para comprender cómo detectar posibles daños y garantizar que la supervisión humana siga siendo un elemento clave del apoyo mediado por la IA.

Además, las funciones basadas en IA (por ejemplo, en entornos de videojuegos, incluidos los personajes controlados por IA, la generación personalizada de contenidos y los chatbots integrados en los juegos) no se abordan plenamente en el marco legislativo vigente para garantizar una protección adecuada de los menores en línea¹⁴⁶.

LA SOLEDAD COMO CAUSA O EFECTO DEL USO

DE LOS MEDIOS SOCIALES

En el caso de los niños y adolescentes, la soledad puede ser una causa o un efecto del uso de los medios sociales¹⁴⁷. En los casos en que la soledad puede considerarse una causa, los sentimientos de aislamiento pueden propiciar un mayor uso de los medios sociales¹⁴⁸ para entablar nuevas amistades. La soledad fuera de línea también puede motivar comportamientos como la presentación poco realista de uno mismo en línea, lo que a su vez puede exacerbar los sentimientos de soledad¹⁴⁹.

De manera más general, experimentar daños en línea puede llevar a los menores a retraerse de las actividades sociales y escolares, a perder la confianza en los demás y a mostrarse más reacios a participar en actividades en línea que promuevan el bienestar (como relacionarse con amigos o acceder a determinados servicios)¹⁵⁰. Es importante reconocer que los daños en línea, incluido el ciberacoso, a menudo se solapan con los daños en el mundo físico.

USO PASIVO FRENTE A USO ACTIVO

El diseño de los medios sociales y otros servicios digitales es otro factor importante que influye en la forma en que estos servicios afectan a la salud mental de niños y adolescentes. Las vías de interacción automatizadas, optimizadas para alcanzar fines comerciales, pueden hacer que los menores se vean expuestos a un flujo aparentemente interminable de contenidos nocivos, desde imágenes gráficas de autolesiones y trastornos alimentarios hasta imágenes de carácter sexual¹⁵¹.

Las investigaciones indican que el modo en que los niños y adolescentes interactúan con los medios sociales influye en los efectos que estos pueden tener en su salud mental y su bienestar. El uso pasivo, como la navegación y el desplazamiento por la pantalla, puede estar asociado a mayores niveles de síntomas depresivos, soledad y estrés¹⁵².

Por su parte, el uso activo, como publicar, comentar, enviar mensajes y dar «me gusta», tiende a correlacionarse con un mayor bienestar, una mayor satisfacción con la vida (especialmente entre las niñas) y una mayor percepción de apoyo social. Sin embargo, algunos resultados son contradictorios en lo que respecta a la relación entre el uso activo y pasivo y la frecuencia de la depresión¹⁵³.

PREOCUPACIONES RELACIONADAS CON LA IMAGEN CORPORAL Y CONDUCTAS ALIMENTARIAS

Las plataformas de medios sociales proporcionan a niños y adolescentes acceso a una amplia variedad de contenidos relacionados con las conductas alimentarias, que abarcan prácticas tanto saludables como poco saludables. Los canales que promueven los trastornos alimentarios suscitan gran preocupación y pueden fomentar conductas alimentarias disfuncionales que dificultan la recuperación¹⁵⁴.

Estos canales pueden utilizar etiquetas que cambian constantemente para evitar la detección y el bloqueo por parte de las plataformas de medios sociales, y que promueven la delgadez, la baja autoestima y el perfeccionismo. Estas conductas están asociadas a trastornos alimentarios que afectan, en particular, a las adolescentes¹⁵⁵ y pueden comenzar a partir de los 10 años.

La amplia difusión y normalización de publicaciones que muestran el «cuerpo perfecto» y de imágenes que promueven el «ideal de delgadez», a menudo a través de actividades centradas en fotografías en los medios sociales, pueden contribuir aún más a la insatisfacción con la propia imagen corporal y a la vergüenza corporal entre niños y adolescentes.

Esta exposición puede dar lugar a una mayor autoobjetivación, a preocupaciones relacionadas con la imagen corporal e incluso al deseo de someterse a cirugía estética. Los adolescentes, especialmente las chicas, corren un riesgo especial de desarrollar percepciones negativas de su propia imagen corporal, perpetuadas por la representación de estándares corporales idealizados en los medios sociales¹⁵⁶.

DESINFORMACIÓN E INFORMACIÓN ERRÓNEA

Los menores tienden a preferir los medios sociales y las plataformas en línea como fuentes de noticias e información frente a los medios de comunicación tradicionales¹⁵⁷. Este uso los expone a una amplia variedad de desinformación e información errónea en línea.

A la edad de 8 años, alrededor de la mitad de los niños afirma encontrarse con información errónea semanalmente¹⁵⁸. A medida que aumenta la edad de los niños, aumenta también la frecuencia con la que declaran haber estado expuestos a información errónea¹⁵⁹. Una encuesta realizada en los Estados Unidos indicó que más de un tercio de los adolescentes han sido engañados por contenidos falsos en línea¹⁶⁰.

Es posible que los niños y adolescentes ni siquiera estén familiarizados con los conceptos de información errónea y desinformación, lo que da lugar a una infranotificación y a una falta de conciencia sobre los riesgos conexos. Esto pone de relieve la brecha existente entre las capacidades cognitivas y emocionales de los niños y los riesgos a los que están expuestos en línea. Si bien alrededor del 70 % de los jóvenes de la UE declararon que podían reconocer con confianza la desinformación en línea¹⁶¹, sus respuestas se ven influidas por su comprensión de lo que constituye desinformación y por otros factores (por ejemplo, el género, el contexto socioeconómico, etc.).

Con la aparición de tecnologías cada vez más sofisticadas capaces de crear y difundir información errónea y desinformación, incluidas las herramientas de IA¹⁶², resulta cada vez más difícil para los usuarios, en particular los menores, distinguir la información poco fiable de la fiable.

Los menores no solo pueden verse directamente perjudicados por la información errónea y la desinformación, sino que también pueden difundirlas entre sus iguales¹⁶³, por ejemplo, para ganar popularidad o recibir confirmación¹⁶⁴. Una tendencia especialmente preocupante es el uso cada vez mayor de los medios sociales por parte de los adolescentes para buscar información sobre cuestiones personales y relacionadas con la salud (mental), a pesar de la prevalencia generalizada de información errónea en línea sobre estos temas¹⁶⁵.

Una investigación periodística realizada en 2021 reveló que, durante los primeros 35 minutos en una plataforma de medios sociales, casi el 90 % de los usuarios había visto información errónea específica sobre las vacunas contra la COVID-19¹⁶⁶. Estos resultados ponen de relieve la necesidad de adoptar medidas de protección para limitar la difusión de información errónea y desinformación en línea.

En los ciclos de evaluación y mitigación de riesgos de las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño, en el marco del Reglamento de Servicios Digitales de la UE, tanto los proveedores como la sociedad civil señalaron riesgos sistémicos para la salud pública derivados de la difusión a gran escala de desinformación e información errónea de carácter médico. Los proveedores de mercados en línea también señalaron riesgos sistémicos derivados de la venta, a través de sus plataformas, de sustancias legales pero nocivas y de productos médicos ilegales, no conformes o no regulados. Otro motivo de preocupación son los contenidos relacionados con las autolesiones, los trastornos alimentarios y las prácticas sanitarias arriesgadas.

Esto subraya la importancia de dotar a los niños y adolescentes, pero también a los cuidadores y educadores, de competencias y alfabetización digitales desde una edad temprana. Los servicios públicos, incluidos los servicios sanitarios, deben reflexionar sobre cómo facilitar a los niños, adolescentes y cuidadores el acceso en línea a información y orientación precisas y adecuadas a la edad sobre cuestiones de salud mental, física, sexual y otras cuestiones relacionadas con la salud¹⁶⁷.

AUTOLESIONES DELIBERADAS Y CONDUCTA SUICIDA

La prevalencia de las autolesiones deliberadas entre los adolescentes es difícil de determinar debido a la escasez de datos sobre la asistencia hospitalaria; sin embargo, las pruebas indican un aumento de su incidencia¹⁶⁸. La Organización Mundial de la Salud (OMS) señala que el suicidio fue la tercera causa principal de muerte entre las personas de 15 a 29 años a escala mundial en 2021, siendo las mujeres de este grupo de edad especialmente vulnerables¹⁶⁹.

El uso de los medios sociales y otros servicios digitales para acceder a contenidos sobre autolesiones deliberadas y compartirlos constituye un problema social. Estas actividades contribuyen a la normalización y desensibilización frente a las conductas autolesivas. Las investigaciones indican que la exposición a contenidos relacionados con las autolesiones o el suicidio en los medios sociales puede dar lugar a los denominados efectos de «contagio» o «Werther»¹⁷⁰. Interactuar con contenidos relacionados con el suicidio y las autolesiones en los medios sociales también puede aumentar la probabilidad de ver contenidos conexos en el futuro debido a la amplificación algorítmica¹⁷¹.

Los adolescentes pueden publicar contenidos relacionados con las autolesiones en los medios sociales para tener una sensación de pertenencia o buscar validación o apoyo. Sin embargo, las reacciones que reciben pueden ser difíciles de gestionar. Si bien pueden ofrecer un apoyo positivo, también pueden reforzar inadvertidamente las conductas autolesivas o suicidas¹⁷². La relación entre la influencia de los medios sociales y la conducta suicida es compleja e incluye asociaciones indirectas y polifacéticas [véase el recuadro sobre el caso «White Tiger»].

La victimización en línea, incluido el ciberacoso, y su potencial para aumentar la sensación de aislamiento de niños y adolescentes se han asociado a una mayor prevalencia de las autolesiones deliberadas y las ideas suicidas¹⁷³. El papel de los medios sociales y otros servicios digitales en estos contextos requiere un examen minucioso para mitigar sus efectos negativos y apoyar de manera eficaz a los niños y adolescentes vulnerables, así como a sus círculos de apoyo.

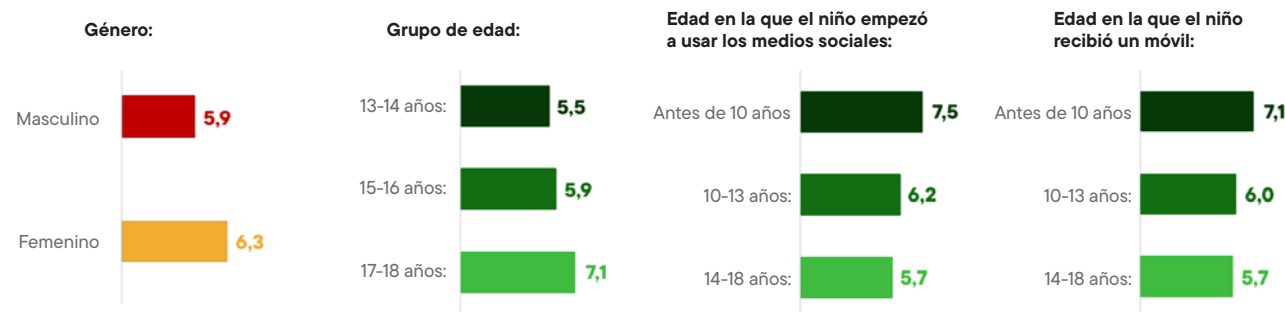
Riesgos para la salud física

La mayoría de los efectos de los medios sociales y otros servicios digitales sobre la salud física están relacionados con el uso de pantallas por parte de los menores en general, más que con tipos específicos de uso, como los medios sociales. Al igual que ocurre con los medios sociales, el tiempo frente a las pantallas no implica necesariamente solo efectos negativos, sino que depende en gran medida de la actividad concreta que se realice. Entre los principales temas de investigación en este ámbito figuran el impacto del tiempo frente a las pantallas en la visión, el desarrollo cerebral, el consumo de alcohol y el sueño de los niños y adolescentes¹⁷⁴.

Los datos del Eurobarómetro sobre el impacto del tiempo excesivo frente a las pantallas y los medios sociales en la salud mental de los jóvenes indican que los adolescentes de entre 13 y 18 años pasan una media de 4,5 horas frente a las pantallas en un día lectivo normal. Durante el fin de semana, esta cifra aumenta hasta una media de 6,1 horas al día y en casi la mitad de los adolescentes (46 %) supera las 6 horas. Durante los fines de semana, el 14 % de los adolescentes supera las diez horas diarias.

Gráfico 1: El aumento del uso de pantallas por parte de los adolescentes durante el fin de semana

Pregunta: ¿Cuánto tiempo pasas en total frente a las pantallas (teléfono inteligente, ordenador, tableta, televisión, consola de videojuegos)^a?



Fuente: Comisión Europea (2026). Encuesta del Eurobarómetro sobre el impacto del tiempo excesivo frente a las pantallas y de los medios sociales en la salud mental de los jóvenes, junio de 2026.

LA VISTA Y LA SALUD FÍSICA

Se reconoce que el uso prolongado de pantallas aumenta el riesgo de dolor de espalda, cefaleas¹⁷⁵ y fatiga ocular digital (también denominada «síndrome visual informático»). El riesgo de experimentar estos síntomas aumenta con un tiempo prolongado frente a las pantallas, problemas de visión no corregidos, un texto de tamaño reducido, una baja resolución, una altura o distancia inadecuadas respecto a la pantalla y una iluminación insuficiente¹⁷⁶.

Los niños son especialmente vulnerables a los problemas de visión causados por el uso prolongado de pantallas, ya que muchos presentan trastornos visuales no diagnosticados o reciben revisiones oftalmológicas de baja calidad¹⁷⁷.

Pasar un tiempo excesivo en los medios sociales y otros servicios digitales también puede suponer un coste de oportunidad, ya que los niños y adolescentes no pueden participar en actividades fuera de línea, como la actividad física y el juego presencial, que son fundamentales para su desarrollo y su salud.

«La mayoría de los riesgos debatidos durante el panel especial sobre seguridad infantil en línea, incluido el tiempo excesivo frente a las pantallas y el uso de aplicaciones de asistentes de IA, son pertinentes no solo para los niños y los jóvenes, sino para personas de todas las edades.»

— ALBERTO MONGE ROFFARELLO,
PROFESOR ADJUNTO DE BIENESTAR
DIGITAL Y DISEÑO ÉTICO DE LA IA,
POLITECNICO DI TORINO

a. Nota: Las cifras representan la media de horas de uso de pantallas al día (durante el fin de semana).

SUEÑO

Otros riesgos frecuentes para la salud física derivados del uso de los medios sociales son la disminución de la actividad física, el tiempo que se pasa al aire libre y la reducción de las horas de sueño¹⁷⁸. Dormir lo suficiente es fundamental para el desarrollo de los niños y adolescentes, la regulación emocional, la consolidación de la memoria, la maduración cerebral y la liberación de la hormona del crecimiento¹⁷⁹. A pesar de ello, una gran proporción de adolescentes no cumple las recomendaciones de sueño para su edad¹⁸⁰.

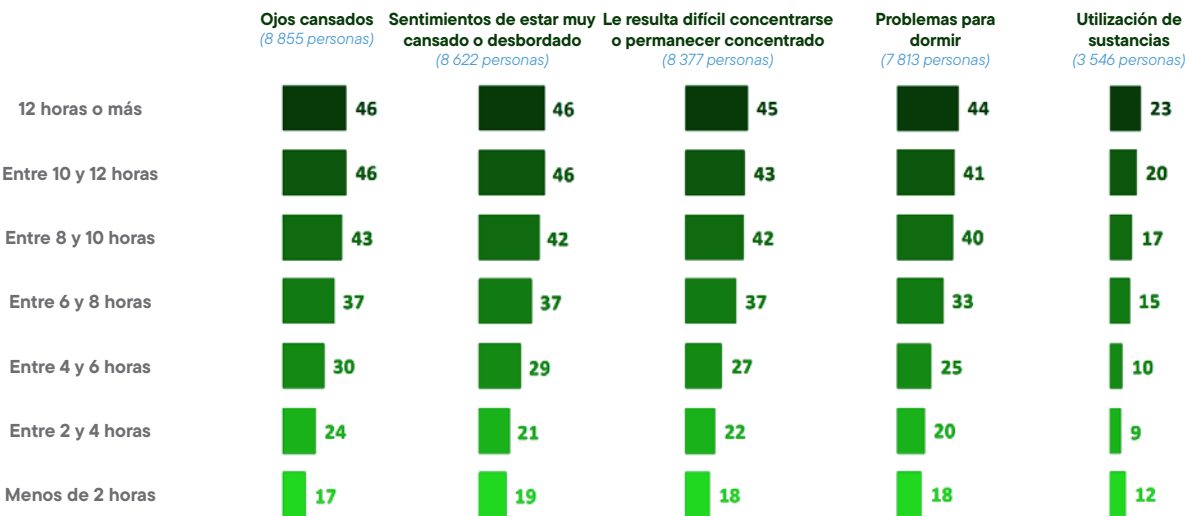
Las pruebas sugieren que el uso de pantallas por parte de niños y adolescentes puede contribuir a una menor duración y una peor calidad del sueño, al restar tiempo de sueño, generar estimulación psicológica y suprimir la producción de melatonina (especialmente debido a la emisión de luz azul)¹⁸¹. El tiempo frente a las pantallas también puede sustituir el tiempo al aire libre, lo que tiene un efecto negativo en el sueño¹⁸² y la salud física y mental general de los menores.

Las encuestas muestran un elevado uso nocturno entre los adolescentes. Los patrones específicos por edad revelan que los niños menores de 5 años están protegidos en gran medida por el control parental. Por su parte, los niños de entre 6 y 12 años presentan una mayor latencia y una peor calidad del sueño, mientras que los de entre 13 y 15 años notifican retrasos en la conciliación del sueño, una menor calidad de este y una mayor activación cognitiva antes de dormir¹⁸³.

Las intervenciones generales destinadas a reducir el tiempo frente a las pantallas (por ejemplo, reducir su uso antes de acostarse, después de las 21:00 horas) han demostrado tener un efecto positivo en la duración del sueño¹⁸⁴ y el estado de alerta al día siguiente¹⁸⁵. Las investigaciones sobre los efectos de una elevada exposición a las pantallas en el desarrollo cerebral de los menores son, en gran medida, de carácter correlacional y no permiten establecer una relación de causalidad.

Gráfico 2: Aumento de los síntomas en adolescentes en función del tiempo frente a las pantallas

Pregunta: ¿Cuál de las siguientes situaciones, en su caso, te ha ocurrido en los últimos treinta días^b?



Fuente: Comisión Europea (2026). Encuesta del Eurobarómetro sobre el impacto del tiempo excesivo frente a las pantallas y de los medios sociales en la salud mental de los jóvenes, junio de 2026.

b. Nota: Las cifras representan el porcentaje (%) de encuestados que señalaron problemas en función del tiempo frente a las pantallas (durante el fin de semana).

DISEÑO ADICTIVO Y «PATRONES OSCUROS»

Según datos de la OMS, más de un tercio de los adolescentes afirma estar en contacto constante con sus amigos en línea. Uno de cada diez adolescentes muestra signos de un uso problemático de los medios sociales, caracterizado por síntomas similares a los de la adicción¹⁸⁶.

Recientemente, la investigación en el ámbito de la medicina de las adicciones ha pasado de centrarse en los factores individuales que dan lugar a conductas adictivas en línea o las caracterizan, a examinar también el diseño de los medios sociales y otros servicios digitales que favorecen dichas conductas. Los niños de entre 6 y 12 años pueden estar expuestos a un riesgo particular de desarrollar conductas adictivas tempranas asociadas al uso de los medios sociales y otros servicios digitales. Estos riesgos persisten, especialmente durante los primeros años de la adolescencia.

Las técnicas de diseño adictivo y los «patrones oscuros»¹⁸⁷ presentes en algunos medios sociales y otros servicios digitales (de forma intencionada o no) distorsionan o merman la capacidad de los usuarios para tomar decisiones autónomas e informadas. Entre las funciones adictivas figuran la reproducción automática de contenidos, el desplazamiento infinito por la pantalla, la ludificación y las funciones de «deslizar para actualizar». Entre los patrones oscuros se incluyen los temporizadores de cuenta atrás falsos, las interfaces web diseñadas para inducir a los consumidores a realizar compras, suscribirse o tomar otras decisiones, y la información oculta¹⁸⁸.

Las investigaciones indican que otras funciones, como el mecanismo «me gusta» y las «notificaciones push», también pueden fomentar conductas compulsivas¹⁸⁹. Los estudios también han señalado que las plataformas diseñadas para maximizar la interacción tienen efectos predominantemente negativos en los adolescentes¹⁹⁰. Debido a sus características de desarrollo y a la importancia de la aceptación por parte de sus iguales en la formación de la identidad, los adolescentes son especialmente susceptibles a estos diseños persuasivos¹⁹¹. Los adultos jóvenes y los adultos con problemas de bienestar preexistentes también son especialmente vulnerables¹⁹².

El control de adecuación en materia de equidad digital de 2024 de la Comisión Europea¹⁹³ reveló que las personas se encuentran con mucha frecuencia en línea con funciones como los patrones oscuros. Se constató que hasta el 97 % de los sitios web y aplicaciones más populares utilizados por los consumidores de la UE usan al menos un patrón oscuro. También se observó que el 31 % de los consumidores pasaba más tiempo y gastaba más dinero en línea debido a diseños adictivos.

Para lograr un cambio sistémico es necesario desplazar el foco de atención de la responsabilidad individual al impacto más amplio de las estrategias de diseño de los medios sociales y otros servicios digitales. Los investigadores están examinando los modelos de negocio basados en datos de las plataformas de medios sociales, que dan prioridad a la interacción con ánimo de lucro, y están debatiendo modelos alternativos que hagan hincapié en un diseño ético¹⁹⁴.

Esto se complementa, en términos más generales, con llamamientos para que el interés superior de los niños sea la consideración principal en el diseño y la gestión de los entornos digitales¹⁹⁵, con el fin de favorecer su bienestar digital.

ABUSO DE ALCOHOL Y DROGAS

A lo largo de la última década, las investigaciones han identificado y estudiado la relación entre el uso de los medios sociales y el consumo de alcohol entre los adolescentes¹⁹⁶. El alcohol está muy presente en los medios sociales, pero existen diferencias importantes entre los distintos servicios digitales en cuanto a su prevalencia y representación¹⁹⁷. Las representaciones positivas del alcohol en los medios sociales influyen en las actitudes y en las normas percibidas¹⁹⁸. La exposición a contenidos relacionados con el alcohol y su difusión se asocian con un mayor consumo de alcohol, lo que crea un bucle de refuerzo bidireccional¹⁹⁹.

Las diferencias individuales, como los rasgos de disposición, el contexto social y la etapa de desarrollo, moderan esta relación. Los entornos familiares pueden amortiguar estos efectos, ya que una socialización negativa respecto al alcohol por parte de los progenitores y los homólogos puede atenuar la influencia de los contenidos relacionados con el alcohol en línea²⁰⁰. Entre las futuras prioridades de investigación figuran ampliar los estudios más allá de las muestras WEIRD^e, aclarar las dinámicas temporales y examinar cómo los distintos tipos de contenido (representaciones positivas, publicidad y mensajes de prevención) interactúan con las conductas de consumo de alcohol de los adolescentes.

En lo que respecta al abuso de drogas, las pruebas indican que en los medios sociales hay una amplia disponibilidad de contenidos que promueven el consumo de drogas o que muestran activamente su consumo. Esto puede influir en las actitudes, los comportamientos y la percepción de los riesgos relacionados con el consumo de drogas, especialmente entre los niños y los adolescentes²⁰¹. Al igual que ocurre con el alcohol, las investigaciones sugieren que los contenidos relacionados con las drogas en los medios sociales se asocian con mayores probabilidades de consumo de cannabis y de varias drogas²⁰².

EXPOSICIÓN A LA DELINCUENCIA Y CONTENIDOS ILÍCITOS EN LÍNEA

Según Europol, los niños y adolescentes están expuestos a diversos delitos en línea, como la captación sexual, el abuso sexual de menores, la radicalización o la captación para actos violentos y terrorismo²⁰³. Estos riesgos se ven agravados por la participación de los menores en los espacios en línea²⁰⁴, así como por su exposición a contenidos nocivos o abusivos, incluido el acceso a pornografía desde una edad muy temprana²⁰⁵.

Las pruebas del contexto alemán indican que el embaucamiento y el abuso sexual de menores en línea son significativamente más frecuentes entre las generaciones jóvenes más recientes. Esto puede deberse a una mayor exposición a los entornos digitales, junto con la proliferación de los medios sociales en las últimas décadas. Estas constataciones ponen de relieve la necesidad de una prevención urgente y específica para abordar los riesgos a los que se enfrentan los niños y adolescentes en línea²⁰⁶.

MATERIAL DE ABUSO SEXUAL DE MENORES

En las últimas décadas, los espacios de los medios sociales y otros servicios digitales se han convertido en un elemento central de la proliferación de material de abuso sexual de menores, así como de su producción, difusión y consumo. En 2025, el 63 % de todas las páginas web de abuso sexual de menores encontradas por la Internet Watch Foundation estaban alojadas en Estados miembros de la UE.

Según datos de 2025 del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) de los Estados Unidos, la captación sexual en línea está aumentando a un ritmo alarmante, con un incremento de las

c. Muestra demográfica occidental, con alto nivel educativo, industrializada, rica y democrática (WEIRD, por sus siglas en inglés).

denuncias del 158 % en los últimos tres años. Los infractores utilizan sistemáticamente los medios sociales, las aplicaciones de mensajería y las plataformas de videojuegos para establecer contacto con menores y llevar a cabo actividades de captación sexual. Estas interacciones en línea se traducen a menudo en explotación fuera de línea, lo que demuestra una estrecha relación entre la captación sexual en línea y la comisión de delitos conexos fuera de línea.

Los avances tecnológicos, incluida la IA generativa, están amplificando los riesgos y acelerando la expansión de posibles abusos. La proliferación de la IA ha dado lugar a un aumento exponencial del material de abuso sexual de menores generado por IA, con un incremento de las denuncias de 5 000 casos en 2023 a 1,3 millones en 2025²⁰⁷.

Tan solo entre 2024 y 2025, el número de vídeos de abuso sexual de menores generados por IA se multiplicó por más de veintiséis. El 65 % se consideró material de categoría A, la forma más grave de abuso. Estos datos ponen de relieve la amenaza que suponen los entornos de los medios sociales y otros servicios digitales y la IA generativa al facilitar la rápida proliferación de material de abuso sexual de menores.

El consumo de material sintético realista puede reforzar intereses sexuales ya existentes. Según una encuesta realizada en 2021 por Protect Children Finland, el 44 % de los 5 171 encuestados afirmó que ver material de abuso sexual de menores los había llevado a plantearse buscar contacto con menores, y el 37 % declaró haberlo intentado²⁰⁸.

Las niñas pueden estar especialmente expuestas a sufrir daños. En 2025, el 97 % de las imágenes de abuso sexual de menores generadas por IA detectadas por la Internet Watch Foundation representaban a niñas²⁰⁹. Las adolescentes de entre 12 y 18 años pueden ser especialmente vulnerables.

La explotación sexual en línea también está estrechamente vinculada a la trata de seres humanos. Los servicios digitales pueden facilitar la captación, el control y la monetización de las víctimas, incluso en operaciones a gran escala que implican abusos retransmitidos en directo. Esta forma de explotación es una de las que más rápido crece a escala mundial, gracias al anonimato. Los daños a las víctimas son graves y duraderos.

Las víctimas señalan consecuencias psicológicas a largo plazo, como ansiedad, vergüenza y un miedo persistente a ser reconocidas²¹⁰. La circulación continuada de material en línea prolonga de manera indefinida la victimización, lo que significa que el daño no cesa una vez que finaliza el abuso inicial.

Un estudio interno del Centro Común de Investigación (JRC) de la Comisión Europea constató que, si bien las plataformas de medios sociales no son los principales alojamientos de material de abuso sexual de menores, pueden utilizarse para difundirlo, a menudo a través de enlaces a sitios externos o canales cifrados.

Los sistemas algorítmicos integrados en las plataformas de medios sociales pueden amplificar los contenidos relacionados con el material de abuso sexual de menores haciendo que sea más fácil de encontrar y más accesible para los usuarios, incluidos los autores y los menores.

Otros contenidos que muestran a menores presentes en las plataformas de medios sociales, aunque no necesariamente material de abuso sexual de menores, pueden ser explotados por los infractores y reforzar los riesgos para los niños y adolescentes. Entre los riesgos para los menores derivados de la exposición a material de abuso sexual de menores figuran daños emocionales y psicológicos, ansiedad, depresión y traumas.

En el caso de los niños y adolescentes que ya han sufrido abusos sexuales, los entornos en línea pueden contribuir al riesgo de revictimización²¹¹. La disponibilidad y circulación continuadas de material de abuso sexual de menores hacen que el abuso pueda revivirse repetidamente mucho después de que haya terminado el delito inicial²¹². A diferencia de muchas formas de victimización fuera de línea, el material digital puede copiarse, redistribuirse y consultarse de forma indefinida, lo que crea una fuente constante de angustia e incertidumbre para las víctimas, que a menudo son conscientes de que las imágenes o vídeos de sus abusos siguen circulando.

Las pruebas sugieren, además, que las personas que han sobrevivido a abusos sexuales durante la infancia pueden ser especialmente vulnerables a experiencias perjudiciales en línea²¹³. El abuso sexual sufrido durante la infancia se ha asociado con una mayor participación en conductas de alto riesgo en línea, una mayor exposición a contenidos sexuales en línea, tasas más elevadas de victimización por ciberacoso y un riesgo elevado de revictimización iniciada a través de internet²¹⁴. Estas vulnerabilidades pueden reflejar el impacto a largo plazo del trauma en el desarrollo psicosocial y en el autoconcepto sexual, más que el comportamiento individual por sí solo²¹⁵.

Gráfico 3: Cuanto más tiempo pasan los adolescentes frente a las pantallas, más contenidos no deseados e ilícitos encuentran

Pregunta: En los últimos tres meses, ¿has visto o experimentado alguna de las siguientes situaciones al utilizar los medios sociales^d?



Fuente: Comisión Europea (2026). Encuesta del Eurobarómetro sobre el impacto del tiempo excesivo frente a las pantallas y de los medios sociales en la salud mental de los jóvenes, junio de 2026.

Por lo tanto, la exposición reiterada en línea a material sexualizado o de carácter explotador puede reforzar los síntomas relacionados con el trauma, interferir en la recuperación y aumentar la probabilidad de una nueva victimización. Al mismo tiempo, la exposición a material de abuso sexual de menores puede contribuir a la normalización de conductas sexuales de carácter explotador entre los menores, lo que aumenta el riesgo de que los niños vulnerables se conviertan en objeto de nuevos abusos o de coacción. Prevenir la difusión de material de abuso sexual de menores no solo es esencial para poner fin a los abusos que

d. Nota: Las cifras representan el porcentaje (%) de encuestados que señalaron riesgos en función del tiempo frente a las pantallas (durante el fin de semana).

continúan produciéndose, sino también para reducir el riesgo de revictimización y apoyar la recuperación a largo plazo de los niños y adolescentes afectados²¹⁶.

Los menores expuestos a este material o captados en los medios sociales y otros servicios digitales corren un mayor riesgo de ser explotados o abusados ellos mismos. La exposición reiterada a material de abuso sexual de menores puede desensibilizar a los menores ante sus efectos nocivos, lo que puede conducir a la normalización de conductas de carácter explotador.

Los niños y adolescentes que han sufrido abusos sexuales con anterioridad corren un mayor riesgo de revictimización en línea. Las pruebas indican que un historial de abuso sexual de menores se asocia con una mayor vulnerabilidad al embaucamiento y el abuso sexual facilitados por la tecnología, lo que subraya la necesidad de adoptar medidas de protección específicas para este grupo²¹⁷.

RADICALIZACIÓN Y CAPTACIÓN PARA ACTOS VIOLENTOS

Y TERRORISMO

Los entornos de los medios sociales y otros servicios digitales desempeñan un papel importante en la radicalización y la captación de menores para cometer actos de terrorismo y extremismo violento. Los medios sociales, los servicios de mensajería cifrada y las comunidades en línea se utilizan para difundir propaganda, crear redes e interactuar directamente con los menores.

El Informe sobre la situación y las tendencias del terrorismo en la UE de 2025 demuestra que casi un tercio de los sospechosos detenidos en la UE en 2024 por delitos relacionados con el terrorismo eran menores o jóvenes adultos²¹⁸. De los 133 jóvenes sospechosos notificados, 70 eran menores de 18 años. La mayoría de los jóvenes sospechosos estaban vinculados al terrorismo yihadista, seguido del terrorismo de extrema derecha y el extremismo violento.

La captación puede comenzar a una edad muy temprana, con casos documentados en los que estaban implicados niños de tan solo 8 o 9 años. Los niños y adolescentes son especialmente vulnerables a las estrategias de captación en línea empleadas por la delincuencia organizada y los grupos terroristas, que a menudo utilizan entornos de videojuegos y foros en línea para atraer a los menores hacia estas actividades.

Las pruebas demuestran que los menores condenados por delitos de terrorismo en la UE pueden experimentar un proceso de autorradicalización en línea, en el que los contenidos impulsados por algoritmos desempeñan un papel clave en el refuerzo de ideas radicales. La exposición habitual a contenidos violentos en línea puede conducir a una peligrosa normalización y a una desensibilización general ante el daño y el sufrimiento humanos²¹⁹.

El caso «White Tiger» [véase el recuadro a continuación] ilustra cómo las plataformas en línea pueden permitir que redes delictivas y particulares atraigan a menores hacia redes de abuso en línea, facilitando su explotación, captación sexual y abuso psicológico.

EL CASO «WHITE TIGER»

El caso «White Tiger» se centra en un sospechoso detenido en Alemania en el verano de 2025 y presuntamente identificado como una figura destacada dentro del grupo extremista nihilista violento en línea «764». Bajo el seudónimo «White Tiger», el sospechoso está acusado de más de 200 delitos cometidos contra más de 30 niños y adolescentes^e. El sospechoso tenía 16 y 19 años de edad, respectivamente, cuando cometió los presuntos delitos.

Entre los presuntos delitos figura la incitación al suicidio de un niño de 13 años procedente de los Estados Unidos, retransmitida en directo por internet en 2022. Otros casos incluyen la captación sexual de menores de entre 11 y 15 años para que se autolesionaran en línea frente a los espectadores y la producción de material de abuso sexual de menores. Se han identificado víctimas en varios países, principalmente Alemania, los Estados Unidos, el Reino Unido y Canadá. Se acusa al sospechoso de haber buscado deliberadamente en línea a niños y adolescentes vulnerables, aislados o con problemas emocionales, incluidas personas que exploraban su identidad LGBTIQ+.

Mediante técnicas rápidas de captación sexual, el sospechoso presuntamente estableció intensos vínculos de dependencia emocional, aislando de forma gradual a las víctimas de sus redes de apoyo en el mundo real. Una vez aisladas, la captación sexual derivó en una forma maliciosa de radicalización hacia ideologías extremistas violentas y tortura psicológica. El juicio contra el sospechoso comenzó en Alemania en 2026. La Fiscalía se enfrenta a dificultades debido a las dimensiones transnacional y virtual del caso.

La red 764 recurre a formas graves de extorsión, amenazas de *doxing* y «luz de gas» para erosionar el sentido de autonomía de las víctimas. Los autores utilizaron sistemáticamente como arma los servicios digitales generales populares entre los menores. Además, se coaccionó a los adolescentes para que ejecutaran órdenes cada vez más peligrosas, grabaran actos degradantes y adoptaran la ideología nihilista del grupo como una forma perversa de validación.

Una característica clave es que a menudo se chantajea a las víctimas para que se conviertan ellas mismas en autores, obligadas por la red a seleccionar, captar y explotar a otros menores. Esta dinámica ilustra el solapamiento entre la victimización y la delincuencia infantil, en la que se utiliza a menores coaccionados para cometer delitos contra otros niños o para incitarlos a autolesionarse. La fluidez ideológica, la combinación de daños en línea y la intensidad gradual de las autolesiones y la violencia, vinculadas a espacios privados en línea, dificultan los esfuerzos por detectar y llevar ante la justicia a las redes extremistas violentas que operan en línea.

EL USO (INDEBIDO) DE DATOS DE MENORES

Los niños y adolescentes se enfrentan a diversos riesgos al utilizar los medios sociales+ en lo que respecta a la forma en que se recogen y utilizan sus datos personales. Una de las principales preocupaciones es la elaboración de perfiles de menores. El comportamiento de los usuarios en los medios sociales y otros servicios digitales suele ser objeto de seguimiento mediante *cookies* y tecnologías de seguimiento similares con diversos fines. El más intrusivo para la privacidad de los propósitos ligados a dicho seguimiento es el seguimiento entre sitios web con el fin de ofrecer publicidad personalizada. Muchas plataformas de medios sociales recogen datos personales no solo a través de *cookies* instaladas en el dispositivo, sino

e. Este juicio aún está en curso. Los delitos expuestos son meras acusaciones y no prejuzgan en modo alguno el resultado del procedimiento judicial.

también mediante el uso de sus propios servidores a una escala que puede suponer una intrusión en la privacidad de los menores. En determinados casos, los proveedores de servicios digitales y los anunciantes pueden recopilar datos de múltiples fuentes diferentes^f.

Estas prácticas permiten a los proveedores obtener una visión completa del comportamiento, las preferencias, los intereses, los movimientos y las actividades en línea de los menores^g. También pueden revelar aspectos privados del estilo de vida o las creencias de un niño o adolescente, aunque los menores no hayan facilitado directamente esta información. La recopilación generalizada de datos puede reducir el control de los menores sobre sus datos y exponerlos a riesgos imprevistos, incluida la presión para realizar compras dentro de las aplicaciones o adquirir servicios adicionales.

Si bien los menores pueden acogerse al derecho incondicional al olvido previsto en el RGPD²²⁰, este derecho debe ser invocado por el menor una vez que el tratamiento ya haya tenido lugar. Naturalmente, esto también requiere que los menores sean capaces de comprender este derecho y cómo invocarlo.

En relación con esto, los menores se enfrentan a riesgos derivados de su uso de los medios sociales y los servicios digitales, que pueden integrar sistemas de recomendación y algoritmos. Estos sistemas suelen basarse en datos de comportamiento y en la actividad de búsqueda para generar contenidos y anuncios personalizados. También pueden dirigir a los menores hacia contenidos nocivos o inadecuados diseñados para fomentar una interacción prolongada. Estas prácticas aumentan la exposición de los niños y adolescentes al riesgo y la posibilidad de que desarrollen conductas compulsivas o adictivas.

En ambos casos, es posible que los menores no comprendan que se están recogiendo sus datos personales, el alcance de la recogida ni para qué se utilizan sus datos. Estas prácticas hacen que sea más difícil determinar si el consentimiento de los niños se dio «libremente», un principio fundamental de lo que constituye consentimiento con arreglo al RGPD.

Otra preocupación es el uso de los datos de geolocalización de los menores, que pueden ser registrados por aplicaciones comunes y cotidianas, como las de movilidad y meteorología, y que a menudo son objeto de comercio por parte de intermediarios de datos a escala mundial. Si se puede rastrear o determinar la ubicación de un niño o adolescente, existe el riesgo de que sus datos personales sean objeto de un uso indebido, con posibles efectos negativos para su seguridad física y su bienestar, tanto en línea como fuera de línea. Aunque el uso de datos de geolocalización suele estar sujeto al consentimiento^h, los menores pueden dar su consentimiento sin supervisión, por ejemplo, al configurar una aplicación descargada en su teléfono, sin que su consentimiento quede validado mediante la verificación de su edad.

Por último, las violaciones de la seguridad de los datos personales pueden tener una serie de efectos adversos para los menores, que pueden dar lugar a daños físicos, materiales o inmateriales²²¹. Esto puede incluir la pérdida de control de los menores sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad, las pérdidas financieras y la inversión no autorizada de la seudonimización. También puede incluir otras desventajas económicas o sociales significativas.

f. Véase, por ejemplo, Meta Platforms Inc/Bundeskartellamt (C252/21).

g. Meta Platforms Inc/Bundeskartellamt (C252/21).

h. En el caso de los datos de geolocalización generados en el contexto de los servicios de telefonía tradicionales (el lugar desde el que se realizó una llamada mediante un teléfono móvil o se envió un SMS), esto se desprende del artículo 9 de la Directiva sobre la privacidad y las comunicaciones electrónicas. En el caso de los datos de geolocalización obtenidos por otros medios (normalmente la función de localización GPS del dispositivo móvil), esto estaría sujeto al RGPD y podría basarse en fundamentos jurídicos diferentes. Sin embargo, teniendo en cuenta el carácter intrusivo de los datos de geolocalización para la privacidad, el antiguo Grupo de Trabajo del artículo 29 y el CEPD consideran que es necesario el consentimiento.

VIDEOJUEGOS

Los videojuegos no solo ofrecen entretenimiento a niños y adolescentes, sino también espacios sociales en los que pueden conectarse y comunicarse con otras personas en línea. Algunas pruebas indican que los videojuegos pueden aportar beneficios en forma de conductas prosociales²²², creación de comunidades y evasión de la realidad²²³. Actualmente se calcula que el 80 % de los menores (entre 2 y 18 años) dedican el 30 % de su tiempo de ocio a jugar a videojuegos²²⁴.

Los videojuegos adoptan formas muy diferentes, lo que presenta diversos riesgos para los menores. Varios de los juegos más jugados ofrecen funciones similares a las de una plataforma. La comunicación abierta a través de estos servicios puede exponer a los menores a riesgos, como el ciberacoso, la captación sexual y la radicalización²²⁵, así como al acceso a contenidos nocivos o inadecuados para su edad. Los denominados «videojuegos intermediarios», por ejemplo, permiten a los usuarios jugar y crear sus propios contenidos o juegos. Los contenidos generados por los usuarios aumentan el riesgo de que los menores se vean expuestos a contenidos inadecuados para su edad.

Algunas plataformas también distribuyen juegos. Tanto los videojuegos como dichas plataformas pueden emplear prácticas comerciales, incluidas las cajas de recompensas, los sistemas de «pagar para avanzar», las compras integradas en la aplicación y las monedas virtuales, que pueden ser manipuladoras y provocar gastos no deseados y conductas compulsivas o adictivas²²⁶. En 2018, el trastorno del juegoⁱ se incluyó en la 11.ª revisión de la Clasificación Internacional de Enfermedades (CIE-11). Parece ser más frecuente entre los adolescentes y los hombres jóvenes de entre 12 y 20 años.

Una encuesta indicó que el 12 % de los adolescentes presentaba riesgo de desarrollar un uso problemático de los videojuegos²²⁷. Estas pruebas también sugieren que los niños de entre 11 y 15 años se enfrentan a un mayor riesgo de uso problemático en comparación con las niñas. Entre los adolescentes, el trastorno del juego se ha asociado con niveles elevados de externalización (como conductas antisociales y problemas de ira) e internalización (por ejemplo, angustia emocional y baja autoestima). Los adolescentes que padecen trastorno del juego pueden estar expuestos a un mayor riesgo de bajo rendimiento académico, abandono escolar prematuro y problemas psicosociales y relacionados con el sueño.

En junio de 2026, el sistema paneuropeo de clasificación por edades de los videojuegos, PEGI, añadió nuevas categorías a sus criterios de clasificación para abordar los riesgos de la interacción en línea en los videojuegos. Los juegos que se presenten a partir de ahora se clasificarán según criterios más amplios que abarcan tanto el contenido como las funcionalidades. Esto incluye las compras de contenidos dentro del juego, los artículos aleatorios de pago, las funciones de comunicación y las que incentivan el juego continuo. Algunas de estas características están ahora vinculadas a categorías de edad específicas, lo que puede utilizarse para evaluar si un videojuego requiere una clasificación por categoría de edad más elevada.

- i. El trastorno del juego se define como un patrón de conducta de juego caracterizado por la reducción del control sobre el juego, el aumento de la prioridad concedida al juego sobre otras actividades, hasta el punto de que el juego prevalece sobre otros intereses y actividades diarias, y el mantenimiento o la escalada de la actividad de juego a pesar de la aparición de consecuencias negativas. Véase: Organización Mundial de la Salud (2020). *Addictive behaviours: Gaming disorder* [«Conductas adictivas: trastorno del juego», disponible en inglés].

Según un representante de la organización alemana «Unterhaltungssoftware Selbstkontrolle» (USK), al menos uno de los nuevos criterios de la USK se ha aplicado a alrededor del 30 % de todos los videojuegos presentados desde que se actualizó el sistema. De ellos, aproximadamente uno de cada tres ha recibido, como consecuencia, una clasificación por categoría de edad más elevada²²⁸.

CARACTERÍSTICAS COMUNES DE LOS MEDIOS SOCIALES+ Y RIESGOS

Los medios sociales y otros servicios digitales difieren ampliamente entre sí, pero comparten una serie de características comunes. La OCDE²²⁹ y los investigadores han desarrollado diferentes clasificaciones de los riesgos a los que pueden verse expuestos los niños y adolescentes en línea. La clasificación 5C ayuda a los proveedores de medios sociales y otros servicios digitales, al mundo académico y a los responsables políticos a comprender y evaluar mejor los riesgos a los que se enfrentan los menores en línea²³⁰.

La clasificación 5C consta de cinco categorías:

- // Riesgos de conducta: riesgos de que los menores participen en conductas nocivas, las presencien o sean víctimas de ellas;
- // Riesgos de contacto: riesgos de que los menores se encuentren con agentes malintencionados en línea o sean objeto de sus acciones;
- // Riesgos de contenido: riesgos de encontrarse con contenidos nocivos;
- // Riesgos de contrato: riesgos de que los menores celebren contratos potencialmente perjudiciales;
- // Riesgos transversales (abreviados como «CC» en el cuadro que figura a continuación): riesgos para la salud, la privacidad y el trato justo (no discriminación) de los menores.

El Centro Europeo para la Transparencia Algorítmica (ECAT)²³¹ ha relacionado las características comunes con los riesgos de la clasificación 5C en una matriz de protección de menores en línea, que se resume en el cuadro que figura a continuación. Es importante señalar que los menores de diferentes edades están expuestos a distintos niveles de riesgo en función de estas características²³².

CARACTERÍSTICAS COMUNES EN LÍNEA Y RIESGOS 5C ASOCIADOS

Elementos	Descripción	Categorías de riesgos (5-C)
Publicidad	Contenidos promocionales mostrados a los usuarios, a menudo para promocionar productos o servicios.	Contenido, conducta, contratos, cc-Salud, cc-Privacidad, cc-Discriminación
Garantía/verificación de la edad	Métodos utilizados para confirmar la edad de los usuarios a fin de garantizar que cumplen los requisitos de edad de la plataforma.	Contenido, cc-Salud, cc-Privacidad, cc-Discriminación
Chatbots de IA	Sistemas automatizados que simulan la conversación con usuarios que utilizan inteligencia artificial.	Contenido, cc-Salud
Filtros de belleza	Herramientas que mejoran o alteran la apariencia de un usuario en fotos o vídeos.	cc-Salud
Observaciones/Opiniones	Comentarios o expresiones de pensamiento sobre contenidos o publicaciones.	Contenido, conducta, contrato, cc-Salud, cc-Privacidad
Prácticas comerciales	Estrategias y actividades utilizadas por los medios sociales y otros servicios digitales para promover y vender productos o servicios.	Conducta
Recomendaciones de contacto	Sugerencias para que los usuarios se conecten con otros usuarios en medios sociales y otros servicios digitales.	Contacto, cc-Salud, cc-Privacidad
Recomendaciones de contenido	Sugerencias facilitadas a los usuarios.	Contenido, cc-Salud, cc-Privacidad, cc-Discriminación
Configuración por defecto	Configuraciones iniciales de los medios sociales y otros servicios digitales que existen cuando un usuario accede a ellos por primera vez.	Contenido, cc-Privacidad
Contenido editorial	Contenidos creados por escritores o editores profesionales para una plataforma en línea.	Contenido
IA generativa	Inteligencia artificial generativa que crea nuevos contenidos o datos.	Conducta, Contenido, cc-Salud, cc-Privacidad
Geolocalización	Utilización de datos para determinar la ubicación física de un usuario.	cc-Salud, cc-Privacidad
Cajas de recompensas	Elementos virtuales que contienen recompensas aleatorias, a menudo adquiridos con dinero real.	Contenido, cc-Salud
Mercados	Medios sociales y otros servicios digitales en los que los usuarios pueden comprar y vender bienes o servicios.	Contenido, conducta, contratos, cc-Salud
Notificaciones	Alertas o mensajes que informen a los usuarios sobre actividades o actualizaciones en la plataforma.	cc-Salud
Interfaz de diseño en línea	Diseño y características de los medios sociales y otros servicios digitales.	cc-Salud
Controles parentales	Herramientas para que los tutores supervisen y gestionen las actividades en línea de los menores.	cc-Salud, cc-Privacidad
Mensajes privados	Las comunicaciones individuales entre usuarios que no son visibles públicamente.	Contacto, Contratos
Presentación de informes y vías de recurso	Mecanismos para que los usuarios señalen y rectifiquen los problemas perjudiciales en una plataforma.	Conducta, Contenido, cc-Privacidad, cc-Discriminación
Condiciones	-	Contrato
Contenido generado por IA	Cualquier forma de contenido, como texto, vídeos, imágenes, reseñas o comentarios, creado y compartido por los usuarios en los medios sociales y otros servicios digitales.	Conducta, Contenido, cc-Salud, cc-Privacidad

Fuente: MANOLIOS, S., *Online Minor Protection Matrix* [«Matriz de protección de menores en línea», disponible en inglés], CHAUDRON, S., SALA, A., y GÓMEZ, E. (editores), Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2026, JRC147657.

Recomendaciones

A pesar de los retos que ello conlleva, las políticas que promueven la seguridad infantil en línea deben diseñarse de una manera orientada a las necesidades y adecuada al desarrollo, que aborde las situaciones y los contextos sociales e individuales complejos y heterogéneos de los niños y adolescentes. En un mundo cada vez más digitalizado, independientemente de que los menores se consideren o no «usuarios activos», a menudo se ven expuestos de forma pasiva a los medios sociales+ por parte de sus principales cuidadores desde los primeros días de vida.

El reto para los responsables políticos es reflejar esta complejidad en políticas específicas, garantizando al mismo tiempo una aplicación y evaluación eficaces. Es fundamental disponer de pruebas sólidas sobre la relación entre los riesgos y los daños y los diferentes medios sociales y otros servicios digitales para fundamentar las medidas adecuadas para proteger y empoderar a los menores en línea. Las características, funcionalidades o formatos específicos utilizados en los medios sociales y otros servicios digitales pueden ser perjudiciales en distinta medida, dependiendo de las circunstancias sociales y personales de un niño o adolescente.

Los menores pertenecientes a grupos raciales, étnicos y religiosos minoritarios, los de origen migrante, los miembros de la comunidad LGBTIQ+, los que tienen necesidades educativas especiales, aquellos con discapacidad o problemas de salud mental preexistentes pueden estar especialmente expuestos a sufrir daños en línea. Esta exposición se ve amplificada por los servicios digitales que integran contenidos o diseños perjudiciales, manipuladores o adictivos. A medida que estas características evolucionan, también deben hacerlo la investigación y la recopilación de pruebas.

Para que esta investigación se materialice, hay un ingrediente clave: datos fiables, procedentes directamente de la fuente, los propios proveedores. Solo mediante el acceso a los datos pertinentes podrán los investigadores, educadores y responsables políticos comprender los riesgos sistémicos, realizar un seguimiento de las amenazas emergentes y diseñar salvaguardias adecuadas.

La UE ha adoptado medidas importantes para garantizar que se facilite la investigación mediante un acceso significativo, proporcionado y efectivo a los datos de las plataformas en línea, en particular en el marco del Reglamento de Servicios Digitales, que facilita el acceso tanto a datos públicos como no públicos para estudiar los riesgos sistémicos que afectan a los menores en línea. Sobre la base de este marco existente y de las medidas que deben adoptar los proveedores [\[véanse también las recomendaciones del capítulo 4\]](#), podrían tenerse en cuenta las siguientes recomendaciones:

«Las recomendaciones sobre el uso de los medios sociales por parte de niños y adolescentes deben basarse en pruebas y en los mejores estudios científicos disponibles.»

— PROF. CHRISTOPH PIEH,
JEFE DEL DEPARTAMENTO DE MEDICINA
PSICOSOMÁTICA Y PSICOTERAPIA,
UNIVERSIDAD DE FORMACIÓN CONTINUA
DE KREMS

RECOMENDACIÓN N.º 1**Basarse en pruebas en ámbitos poco estudiados para reforzar la elaboración de políticas basadas en datos contrastados**

Los investigadores deben seguir basándose en pruebas relativas a los riesgos y oportunidades relacionados con el uso de los medios sociales+ por parte de niños y adolescentes en ámbitos poco estudiados. Entre los ámbitos clave que deben reforzarse figuran los efectos heterogéneos del uso de los medios sociales+ por parte de los menores a lo largo de todo su desarrollo, el uso de dinero en línea por parte de los menores (también en los mercados en línea), las herramientas de IA (incluidos los asistentes de IA) y el diseño ético de los medios sociales+. Los estudios controlados de usuarios en medios sociales y servicios digitales específicos son importantes para investigar el impacto de determinadas características de diseño o de un grupo de ellas. Para aclarar los efectos causales de determinadas características, deben ponerse en marcha ensayos aleatorios controlados. Los proveedores tienen la importante responsabilidad de facilitar estos estudios, proporcionando acceso a investigadores independientes.

Los posibles efectos positivos del uso de los medios sociales+, por ejemplo, en entornos estructurados de cuidado o educativos, constituyen otro ámbito que debe estudiarse más a fondo. También deben examinarse con mayor detalle los factores sociales e individuales que influyen en el impacto del uso de los medios sociales+ en el desarrollo de los menores, así como la interacción entre dichos factores. Estos conocimientos son necesarios para fundamentar y reforzar la elaboración de políticas basadas en datos contrastados que promuevan la seguridad y el empoderamiento de los menores en línea.

RECOMENDACIÓN N.º 2**Los proveedores deben implicar activamente a expertos académicos independientes en el diseño de estrategias y herramientas de mitigación de riesgos**

Más allá del cumplimiento de las normas aplicables, los proveedores de medios sociales y otros servicios digitales deben implicar activamente a expertos independientes y a menores en el diseño de sus estrategias y herramientas de mitigación de riesgos, así como a la hora de desarrollar funciones y servicios específicos para menores en línea. Deben estar representados los conocimientos especializados de una amplia gama de disciplinas y el uso de diversas metodologías para garantizar unos conocimientos sólidos y bien fundamentados.

RECOMENDACIÓN N.º 3**Hay que poner a disposición financiación a largo plazo para la investigación longitudinal europea a gran escala y seguir apoyando los ensayos aleatorios de control**

Ejemplos como el North American Adolescent Brain Cognitive Development (ABCD) Study [«Estudio sobre el desarrollo cognitivo cerebral en adolescentes de América del Norte» (ABCD, por sus siglas en inglés)] podrían inspirar la investigación longitudinal europea a gran escala relacionada con la seguridad infantil en línea. La disponibilidad de pruebas longitudinales europeas a gran escala (que abarquen un período de diez años o más) es importante para apoyar un enfoque neurobiológico y de desarrollo de

la seguridad infantil en línea. Esto ayudaría a abordar las lagunas en las conclusiones en gran medida correlativas en el contexto europeo relacionadas con el impacto del uso de los medios sociales+ en el desarrollo de los menores, su salud física y mental y su exposición a daños por su actividad en línea.

Los ensayos aleatorios controlados también son fundamentales para reforzar la base empírica de las políticas. La financiación de la investigación debe apoyar explícitamente los enfoques de desarrollo y psicopatología que investigan la susceptibilidad de los menores a los riesgos en línea, influidos por factores sociales e individuales en la infancia y la adolescencia.

RECOMENDACIÓN N.º 4

Invertir en infraestructuras de investigación europeas seguras y compartidas para permitir un acceso seguro a los datos de los menores

La Unión Europea y sus Estados miembros deben invertir en infraestructuras de investigación europeas seguras y compartidas, basadas en los principios rectores FAIR [véase más adelante], que permitan a los investigadores y a los responsables políticos acceder también a datos sensibles y no públicos sobre la protección de los menores en línea, respetando plenamente la legislación aplicable en materia de privacidad y protección de datos.

Las infraestructuras compartidas deben integrar los principios rectores FAIR (fáciles de encontrar, accesibles, interoperables y reutilizables)^j para la gestión y administración de los datos científicos a fin de garantizar la solidez, fiabilidad y reutilizabilidad de los datos y la investigación. Colaborar con la comunidad de investigación para garantizar la mejora continua y la disponibilidad de los datos, así como el uso de innovaciones metodológicas.

Debe animarse a los proveedores de medios sociales y otros servicios digitales a que contribuyan al desarrollo de infraestructuras de investigación compartidas para reforzar la base empírica de las medidas de protección de los menores en línea.

RECOMENDACIÓN N.º 5

Reforzar la aplicación de las normas sobre el acceso de los investigadores a los datos y su control

El acto delegado de julio de 2025 relativo al artículo 40 del Reglamento Delegado de Servicios Digitales ha abierto, en principio, una nueva vía para que los investigadores autorizados accedan a los datos de las plataformas en línea. Estos datos pueden utilizarse para llevar a cabo investigaciones que contribuyan a la detección, identificación y comprensión de los riesgos sistémicos, así como a la evaluación de las medidas de mitigación de riesgos que promueven la seguridad infantil en internet.

j. Los principios rectores FAIR para la gestión y administración de datos científicos se introdujeron en 2016 en una publicación de la revista *Scientific Data*. Los principios tienen por objeto mejorar la infraestructura de apoyo a la reutilización de datos académicos mediante el refuerzo de la capacidad de las máquinas y de las personas para encontrar y utilizar datos. Véase: Wilkinson, M.D., et al. (2016). *The FAIR Guiding Principles for scientific data management and stewardship* [«Los principios rectores FAIR para la gestión y administración de datos científicos», documento en inglés]. Datos científicos, 3.

Que esta vía cumpla su cometido depende del cumplimiento por parte de los proveedores de medios sociales y otros servicios digitales y de la aplicación efectiva por parte de las autoridades reguladoras. También se basa en la extensión de los servicios cubiertos y en la calidad y continuidad de los datos facilitados. La Comisión debería evaluar el funcionamiento operativo de los requisitos del acceso a datos y el escrutinio del artículo 40 tras la experiencia inicial de los investigadores al amparo del acto delegado. Esto es fundamental para garantizar que las plataformas en línea hagan un seguimiento de las solicitudes de acceso a los datos con fines de cumplimiento, evaluación de riesgos e investigación.

Las obligaciones de acceso a los datos no solo son un elemento clave del conjunto de instrumentos de transparencia del Reglamento de Servicios Digitales, sino que también forman parte de las responsabilidades más amplias de mitigación de riesgos de los proveedores de medios sociales y otros servicios digitales. También debe alentarse a las plataformas más pequeñas a que permitan a los investigadores acceder a los datos, teniendo en cuenta los riesgos que estas plataformas plantean para los menores y el papel del escrutinio independiente a la hora de abordar estos riesgos. El uso de los principios rectores FAIR para la gestión y administración de datos científicos debe ser la norma en la aplicación del artículo 40.

03

Protección de los menores en un entorno de medios sociales y otros servicios digitales en rápida evolución

En el capítulo anterior se analizaron los diversos riesgos a los que se ven expuestos los niños y adolescentes como consecuencia del uso de los medios sociales y otros servicios digitales para su salud mental y física y su bienestar, y cómo estos riesgos se entrecruzan con factores sociales e individuales para aumentar la exposición de los menores a posibles daños.

En el presente capítulo se examina cómo la legislación y las herramientas de las que disponen actualmente la UE y sus Estados miembros abordan estos riesgos y refuerzan la seguridad infantil en línea.

Este análisis se basa en los pilares tercero y cuarto de los seis principios rectores presentados por los copresidentes para orientar los esfuerzos destinados a mejorar la seguridad infantil en línea: la protección de la infancia, la responsabilidad de los proveedores de medios sociales y otros de servicios digitales, y los derechos de los consumidores. Este capítulo comienza examinando los principales instrumentos legislativos y herramientas de que disponen la UE y los Estados miembros, destacando ejemplos de su aplicación satisfactoria hasta la fecha.

Los principales instrumentos legislativos de la UE en el ámbito de la seguridad infantil en línea constituyeron uno de los puntos de partida clave para la reflexión de los copresidentes sobre cómo reforzar la protección de los menores en línea. La comprensión del contenido y el alcance de las herramientas más potentes a escala de la UE y la detección de lagunas en la legislación o en su aplicación también fueron algunos de los principales temas debatidos en las reuniones del panel especial.

Es ampliamente reconocido que la UE ha establecido un sólido marco legislativo, pero las tecnologías se desarrollan rápidamente, los modelos de negocio se adaptan, surgen nuevas funcionalidades y los reguladores deben adaptarse en consecuencia, ya sea para hacer cumplir la normativa vigente o para subsanar las lagunas existentes. La protección de los menores en un entorno de medios sociales+ en rápida evolución requiere una evaluación y atención constantes para no quedarse atrás.

En la sección «Asuntos pendientes», se determinan varios ámbitos en los que es necesario reforzar los instrumentos y herramientas existentes. El capítulo concluye con la presentación de una serie de reco-

mendaciones sobre cómo reforzar la aplicación de estos instrumentos existentes y cómo abordar mejor las prácticas nocivas y las características y funcionalidades implantadas por los medios sociales y otros servicios digitales para reforzar la protección infantil en línea.

La necesidad de una protección infantil en línea adaptada a la edad

Tal como se analiza en el capítulo 1, un enfoque eficaz de la seguridad infantil en línea debe basarse en la comprensión de que el desarrollo de los niños y adolescentes se produce por etapas. En diferentes momentos a lo largo de su camino hacia la edad adulta, los menores están especialmente expuestos a riesgos específicos. La evolución de las capacidades de los niños y adolescentes determina, en parte, la medida en que están preparados para hacer frente a estos riesgos.

Este análisis toma como punto de partida los respectivos marcos internacionales y de la UE en materia de derechos del niño^a. Las medidas destinadas a promover la seguridad infantil en línea deben basarse en el reconocimiento de los derechos de los niños. Los instrumentos de protección infantil también deben reflejar mejor la evolución de las funciones de los cuidadores y los educadores a la hora de supervisar el uso que hacen los menores de los medios sociales y otros servicios digitales.

El creciente impulso político para restringir el acceso y el uso por parte de los niños y adolescentes de los medios sociales y otros servicios digitales potencialmente nocivos es un paso en la dirección correcta para configurar un enfoque de la seguridad infantil en línea más sensible al desarrollo. Los primeros resultados de los países que han introducido prohibiciones generales por edad para acceder a los medios sociales (por ejemplo, Australia) muestran que la mayoría de los menores encuentran la manera de eludir estas políticas²³³.

Al mismo tiempo, algunos menores se han apartado de los medios sociales+ de riesgo y ahora disponen de más tiempo para actividades fuera de línea (como el deporte y las interacciones sociales en persona). Esto demuestra que el cambio progresivo en torno a las normas de uso de los medios sociales y otros servicios digitales por parte de los menores no solo es posible sino que debe reconocerse.

Sin embargo, siguen existiendo varios retos para aplicar con éxito las restricciones de edad con el fin de reforzar la protección de los menores en línea y permitirles aprovechar las oportunidades que ofrece el mundo digital. Estos retos se analizan más adelante en este capítulo, en la sección «Asuntos pendientes».

Garantizar características de diseño seguras en línea

Cada vez hay más pruebas que demuestran los efectos potencialmente nocivos del uso de los medios sociales y otros servicios digitales por parte de los menores, tal como se analiza en el capítulo 2. Los riesgos a los que se enfrentan los niños y adolescentes en los entornos de los medios sociales+ no son fortuitos. En muchos casos, son el resultado de decisiones deliberadas de los proveedores de medios sociales y otros servicios digitales, orientadas a maximizar la interacción de los usuarios, incluidos los menores, que pueden acceder fácilmente a dichos servicios. La continua evolución de los medios sociales

a. En particular, la Convención de las Naciones Unidas sobre los Derechos del Niño y las Observaciones generales del Comité de los Derechos del Niño, la Carta de los Derechos Fundamentales de la Unión Europea y la Estrategia de la UE sobre los Derechos del Niño.

y otros servicios digitales para captar y mantener la interacción de los usuarios se ha convertido en un elemento central de los modelos de negocio de muchos proveedores.

Cada vez hay más llamamientos para que los reguladores apliquen un enfoque basado en el riesgo y aborden los riesgos inherentes, incluido el uso adictivo o compulsivo, que determinadas características y funcionalidades plantean para los niños y adolescentes, a fin de garantizar que los medios sociales y otros servicios digitales sean «seguros desde el diseño». A pesar de los numerosos ejemplos de medidas de ejecución eficaces para abordar estas cuestiones, los reguladores a menudo se encuentran «a la defensiva».

En la actualidad, los reguladores suelen tener que demostrar que determinadas características y funcionalidades son perjudiciales después de que se hayan implantado en el mercado único y de que, potencialmente, las hayan utilizado millones de niños y adolescentes. Los proveedores de medios sociales y otros servicios digitales deben asumir una mayor responsabilidad a la hora de garantizar y demostrar que las características de sus servicios no son perjudiciales antes de ponerlas a disposición de los menores.

Por lo tanto, podría convertirse en norma que los proveedores de medios sociales y otros servicios digitales que lancen, gestionen o actualicen servicios que puedan plantear riesgos para los niños y adolescentes deban demostrar, antes de la implantación en el mercado, que sus servicios o nuevas funcionalidades son seguros para que los menores los utilicen. La protección de los niños y adolescentes debe formar parte integrante de la arquitectura de los medios sociales+ y ser una norma clave desde el principio de su desarrollo y diseño.

**«Ningún juguete,
medicamento o vehículo
llega a los niños
sin una evaluación
independiente previa
a su comercialización;
los productos
digitales son la
excepción más
evidente, pues solo
se examinan una vez
que el daño ya es
visible.»**

— ALEX COONEY,
DIRECTORA GENERAL Y COFUNDADORA,
CYBERSAFEKIDS

Reforzar la ejecución y la evaluación

Por último, pero no por ello menos importante, debe reforzarse la aplicación de la legislación vigente a escala nacional y de la UE. La UE cuenta con uno de los marcos normativos más avanzados del mundo, que puede utilizar para garantizar que los menores puedan navegar por el mundo en línea con seguridad y confianza. Sin embargo, la eficacia de estas normas depende de su aplicación. Es necesario subsanar las lagunas en la legislación vigente y reforzar la cooperación entre los reguladores a escala nacional y de la UE.

Es posible que se necesiten recursos adicionales para mejorar la capacidad de ejecución. La evaluación de los instrumentos existentes es esencial para garantizar que la legislación y su aplicación arrojen resultados. La sociedad civil y los investigadores tienen que hacer importantes contribuciones a este respecto.

Su papel debe reforzarse para garantizar que la legislación se diseñe y aplique de manera eficaz con el fin de alcanzar el objetivo de permitir que los niños y adolescentes crezcan de forma segura en línea.

Legislación vigente de la UE

En la siguiente sección se examinan la legislación vigente de la UE y las herramientas de que disponen la UE y los Estados miembros para proteger a los menores^b en línea. Este análisis se centra en la legislación de la UE que, a juicio de los copresidentes del panel especial, requiere un mayor refuerzo o una mejor aplicación. Por supuesto, hay muchos instrumentos importantes que no se analizan en detalle en este capítulo, pero que constituyen una parte esencial de la política actual de la UE.

Entre ellos destacan, en particular, la Decisión Marco de 2008 relativa a la lucha contra el racismo y la xenofobia, la Directiva sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, la Directiva relativa a las garantías procesales de los menores sospechosos o acusados en los procesos penales, la Directiva sobre los derechos de las víctimas y la Recomendación de la Comisión sobre sistemas integrados de protección de la infancia.

Las políticas preventivas, como la educación y la alfabetización digitales (incluida la alfabetización en materia de IA), la educación para el bienestar y el apoyo a los menores, los cuidadores y los educadores, se examinan en el capítulo 4, que se centra en el empoderamiento de los niños y adolescentes en línea.

REGLAMENTO DE SERVICIOS DIGITALES Y DIRECTRICES

SOBRE LA PROTECCIÓN DE LOS MENORES

El Reglamento de Servicios Digitales establece normas plenamente armonizadas para la prestación de servicios intermediarios a fin de crear un entorno en línea seguro, predecible y digno de confianza en el que se respeten los derechos de los usuarios, en particular de los menores. El Reglamento de Servicios Digitales se adoptó en 2022 y es plenamente aplicable a las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño^c desde el 25 de agosto de 2023. El Reglamento de Servicios Digitales es plenamente aplicable a todos los demás servicios incluidos en su ámbito de aplicación desde el 17 de febrero de 2024.

En un contexto de auge de los servicios digitales, que se han convertido en una parte importante de nuestra vida cotidiana en la era digital, el Reglamento de Servicios Digitales desarrolla los principios fundamentales consagrados en la Directiva sobre el comercio electrónico desde 2000 para abordar los nuevos riesgos y retos a los que se enfrentan actualmente los menores en línea y promover un comportamiento responsable por parte de los proveedores de servicios digitales.

En última instancia, el Reglamento de Servicios Digitales pretende crear un entorno en línea en el que todas las personas puedan disfrutar de sus derechos fundamentales. Esto incluye la imposición de obligaciones a las plataformas en línea para garantizar un alto nivel de privacidad, seguridad y protección de los menores en línea²³⁴.

b. Nota: En las siguientes secciones de este capítulo, los términos «niños» y «menores» aparecen tal como se utilizan en instrumentos legislativos específicos.

c. En virtud del Reglamento de Servicios Digitales, las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño se definen como servicios con más de 45 millones de usuarios activos al mes en la UE.

Ámbito de aplicación

En concreto, el Reglamento de Servicios Digitales regula a los prestadores de servicios intermediarios. Se trata de servicios digitales que facilitan el alojamiento de contenidos de terceros y las interacciones en línea. La definición de servicios intermediarios abarca a los prestadores que se limitan a transmitir información (por ejemplo, los prestadores de servicios de internet), los servicios de «memoria caché» (transmisión de información con almacenamiento temporal), incluidos los operadores de redes; y el alojamiento de datos a petición de los usuarios (por ejemplo, proveedores de servicios en la nube y plataformas en línea).

A modo de ejemplo, los servicios intermediarios incluyen todas las plataformas en línea, como los mercados en línea, los medios sociales, los juegos en línea o los videojuegos en los que los usuarios pueden jugar y crear sus propios contenidos (a menos que estas funciones sean solo «complementos» menores de un videojuego ya existente), las tiendas de aplicaciones, los sitios de intercambio y emisión en continuo de vídeos, y las plataformas en línea en las que los usuarios pueden ver, publicar y compartir contenidos.

El Reglamento de Servicios Digitales no se aplica a los servicios o funciones de mensajería privada o directa (interpersonal), ni a los servicios digitales sin función de intermediario^d. A fin de garantizar la proporcionalidad, algunas de las obligaciones que el Reglamento de Servicios Digitales impone a las plataformas en línea no se aplican a los proveedores de plataformas en línea que se consideren microempresas o pequeñas empresas debido a sus ingresos y número de empleados. Esta excepción no se aplica si estos servicios se clasifican como plataformas en línea de muy gran tamaño habida cuenta del número de usuarios.

Garantía de cumplimiento

El Reglamento de Servicios Digitales faculta a la Comisión para iniciar investigaciones formales contra las plataformas más grandes sobre la base de una amplia gama de riesgos para los menores, al tiempo que mantiene la flexibilidad necesaria para reaccionar ante nuevos riesgos y avances tecnológicos. Las investigaciones deben respetar en todo momento las garantías procesales y todas las demás garantías jurídicas necesarias para las empresas.

Habida cuenta de las normas plenamente armonizadas del Reglamento de Servicios Digitales, que es un Reglamento directamente aplicable, los Estados miembros de la UE no pueden adoptar ni mantener legislación nacional que duplique el Reglamento de Servicios Digitales o imponga obligaciones a los prestadores de servicios intermediarios. Esto incluye la imposición de obligaciones de verificación de la edad a las plataformas en línea.

Esto afectaría a la aplicación directa y uniforme de las normas en todo el mercado único. No obstante, la legislación nacional, de conformidad con el Derecho de la Unión, puede establecer una edad mínima para acceder a determinados productos o servicios, como también se indica en las directrices de la Comisión sobre la protección de los menores.

La aplicación del Reglamento de Servicios Digitales se basa en un sistema de competencias compartidas de supervisión y garantía del cumplimiento entre los niveles nacional y de la UE. En el caso de las

d. La «función de intermediario» se refiere a los servicios que facilitan el acceso a contenidos de terceros entre los distintos destinatarios de dicho servicio. Algunos ejemplos de servicios no intermediarios serían los minoristas en línea, muchos videojuegos que no implican interacciones con terceros ni la creación de contenidos, o sitios web o aplicaciones individuales.

plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño (véase más adelante), la Comisión tiene competencias exclusivas para supervisar a estos prestadores.

Plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño

En virtud del Reglamento de Servicios Digitales, se aplican obligaciones adicionales a las plataformas en línea de muy gran tamaño y a los motores de búsqueda en línea de muy gran tamaño^e, dado su amplio alcance e influencia. Estas obligaciones responden a las preocupaciones sobre los riesgos generalizados que estos servicios pueden acarrear, lo que va acompañado del más alto nivel de diligencia debida.

En virtud del Reglamento de Servicios Digitales²³⁵, las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño deben detectar, evaluar y mitigar de forma proactiva los riesgos sistémicos reales y previsibles derivados de la prestación de sus servicios, incluidos los riesgos que afectan a los menores. En el caso de las plataformas con menos de 45 millones de usuarios mensuales, las autoridades nacionales del Estado miembro de la UE en el que esté establecida la empresa son responsables de hacer cumplir el Reglamento de Servicios Digitales.

Las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño deben adoptar medidas razonables, proporcionadas y eficaces para mitigar los riesgos detectados. Esto puede incluir la adaptación del diseño, las características y el funcionamiento de sus servicios, así como la adaptación de los sistemas algorítmicos utilizados como parte de sus servicios. Las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño deben ofrecer a los usuarios al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles.

Dada la necesidad de garantizar la verificación por parte de expertos independientes, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben rendir cuentas, mediante auditorías independientes, de su cumplimiento de las obligaciones en virtud del Reglamento de Servicios Digitales.

Directrices del Reglamento de Servicios Digitales sobre la protección de los menores

Las directrices del Reglamento de Servicios Digitales sobre la protección de los menores establecen el marco de referencia para garantizar que todas las plataformas en línea accesibles a los menores ofrezcan un alto nivel de privacidad, seguridad y protección a los menores que utilizan sus servicios.

Las principales medidas recomendadas en las directrices son las siguientes:

- // Configurar por defecto las cuentas de los menores al máximo nivel de privacidad, seguridad y protección, por ejemplo, en lo que respecta a la geolocalización y las recomendaciones de otras cuentas.
- // Establecer una verificación de la edad cuando determinados productos o servicios planteen un riesgo elevado para los menores (por ejemplo, el acceso a contenidos pornográficos) y dichos riesgos no puedan mitigarse con medidas menos restrictivas. Definir claramente lo que la plataforma considera

e. Para consultar la lista completa de plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño designados, véase: Comisión Europea (2026). [Supervisión de las plataformas en línea y los motores de búsqueda de muy gran tamaño designados en virtud del Reglamento de Servicios Digitales](#).

contenidos y comportamientos nocivos para los menores. Esto incluye cualquier contenido y comportamiento que sea ilícito con arreglo a la legislación nacional o de la UE. Comunicar información sobre estas normas y expectativas. Establecer políticas y procedimientos de moderación que definan cómo se detectan y moderan los contenidos y comportamientos para limitar la exposición de los menores a los mismos.

- // Impedir que cuentas desconocidas se pongan en contacto con menores y ocultar su información personal, sus datos y sus contenidos en los medios sociales a cuentas con las que no estén conectados. A modo de ejemplo, dos plataformas en línea de muy gran tamaño designadas han configurado automáticamente como privados los perfiles de los usuarios menores de 16 años. Esto significa que los vídeos que suben solo pueden ser vistos por las personas que ellos aprueben.
- // Prohibir que las cuentas descarguen o hagan capturas de pantalla de contenidos publicados por menores para evitar la extorsión sexual.
- // Modificar los sistemas de recomendación para reducir el riesgo de que los menores se encuentren con contenidos nocivos o se vean atrapados en los denominados efectos de «madriguera de conejo», en los que los menores se ven expuestos a cadenas prolongadas de contenidos relacionados con trastornos alimentarios, autolesiones o suicidio.
- // Establecer salvaguardias en torno a los chatbots de IA integrados en las plataformas en línea. Advertir a los menores de que las interacciones con una función de IA son diferentes de las interacciones humanas y de que la información facilitada por dichas funciones puede ser inexacta o engañosa.
- // Introducir medidas para mejorar las herramientas de moderación. Garantizar que los mecanismos de denuncias, observaciones y reclamaciones de los usuarios sean eficaces, visibles, adaptados a los niños y fácilmente accesibles. Asegurarse de que dichos mecanismos permitan informar y formular observaciones sobre todos los elementos pertinentes de la experiencia de los menores en la plataforma.
- // Establecer requisitos mínimos para las herramientas de control parental. Estas herramientas deben ser adecuadas a la edad y fáciles de utilizar, acceder y activar. También deben ser interoperables y eficaces y no restringir de manera desproporcionada los derechos de los menores a la privacidad o al acceso a los servicios.

«Hacer que las directrices del artículo 28 del Reglamento de Servicios Digitales sean obligatorias para los proveedores de servicios digitales. Esto sería eficaz, legítimo, coherente con la legislación y la normativa vigentes y, lo que es más importante, un medio crucial para respetar los derechos de los niños en el entorno digital.»

— SONIA LIVINGSTONE,
PROFESORA DE LA LONDON SCHOOL OF
ECONOMICS AND POLITICAL SCIENCE
Y MIEMBRO DE LA RED EU KIDS ONLINE

- // Introducir herramientas de apoyo a los usuarios. Esto incluye mensajes de advertencia directamente visibles, enlaces a líneas de apoyo pertinentes u otras fuentes cuando los menores busquen, suban, generen, compartan y reciban contenidos potencialmente ilícitos. También podrían implantarse opciones para mantener el control de la experiencia de los menores mediante la restricción de las interacciones y los contactos.
- // Garantizar la protección de los menores frente a prácticas de explotación económica. Los menores no deben verse expuestos a prácticas y técnicas que puedan provocar gastos excesivos o no deseados o conductas adictivas (por ejemplo, las «cajas de recompensas» de pago).
- // Establecer prácticas de gobernanza, incluidas políticas internas, procesos, funciones y responsabilidades, para fomentar una cultura de seguridad para los menores en su servicio.
- // Garantizar que toda la información, las advertencias y cualquier otra comunicación estén adaptadas a los niños, sean adecuadas para su edad, fáciles de entender y accesibles para todos los menores y se presenten de forma clara y en el punto de uso pertinente. De manera más general, en virtud del Reglamento de Servicios Digitales, todos los usuarios, incluidos los menores, están protegidos por unos requisitos mínimos (por ejemplo, las plataformas en línea deben hacer que sus condiciones generales sean comprensibles en la lengua local de la UE, de modo que los usuarios, incluidos los menores, sean conscientes de las condiciones generales que aceptan).

Un enfoque basado en el riesgo

Las directrices del Reglamento de Servicios Digitales adoptan un enfoque basado en el riesgo, ya que las diferentes plataformas en línea pueden plantear diferentes tipos o niveles de riesgo para los menores. Las directrices reconocen que estos riesgos pueden variar en función del tamaño, el alcance y el tipo de plataforma, su naturaleza, su uso previsto o actual, sus características y su base de usuarios, así como su impacto en los derechos de los niños y otros derechos y libertades. Las plataformas deben tener en cuenta estos factores a la hora de aplicar las directrices.

En consonancia con este enfoque basado en el riesgo, las directrices establecen la manera en que los proveedores deben cumplir las obligaciones de ofrecer un alto nivel de privacidad, seguridad y protección a los menores de manera proporcionada y adecuada. Los proveedores deben tener en cuenta el impacto de las medidas de protección que adopten en los derechos de los niños y otros derechos y libertades, basando dichas medidas en las normas más estrictas disponibles, así como en la perspectiva y los derechos de los niños. En este contexto, debe aplicarse el principio de precaución cuando haya indicios de que una práctica, característica o elección de diseño plantea riesgos para los niños, hasta que existan pruebas de que no son perjudiciales.

Prohibiciones específicas en virtud del Reglamento de Servicios Digitales

En lo que respecta a la publicidad, el Reglamento de Servicios Digitales prohíbe a los proveedores de plataformas en línea presentar anuncios basados en la elaboración de perfiles utilizando los datos personales de menores cuando tengan conocimiento, con una certeza razonable, de que el destinatario del servicio es un menor.

El Reglamento de Servicios Digitales también prohíbe los «patrones oscuros». Esto se refiere a la forma en que se diseñan las interfaces en línea para persuadir o manipular a los usuarios para que tomen determinadas decisiones contrarias a sus intereses. La prohibición de los patrones oscuros se aplica en

situaciones que aún no están previstas en la legislación en materia de protección de los consumidores (la Directiva sobre las prácticas comerciales desleales) y las normas de protección de datos [el Reglamento General de Protección de Datos (RGPD)].

Alertadores fiables

El Reglamento de Servicios Digitales también facilita la denuncia de contenidos (como el discurso de odio ilegal y el material de abuso sexual de menores) y bienes ilícitos por parte de los usuarios al exigir sistemas de alerta fáciles de usar, también para los menores. Las organizaciones de la sociedad civil, expertas en la detección de determinados tipos de contenidos ilícitos en línea, pueden obtener la condición de «alertadores fiables».

Las notificaciones de los alertadores fiables sobre contenidos ilícitos a las plataformas se tratan con carácter prioritario. En la actualidad, más de 70 organizaciones han sido designadas como alertadores fiables por los coordinadores de servicios digitales, y representan ámbitos de especialización que van desde la protección de los menores en línea, las estafas y el fraude, hasta la lucha contra los productos falsificados.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

El Reglamento General de Protección de Datos (en lo sucesivo, el «RGPD») adopta un enfoque basado en el riesgo para el tratamiento de datos personales. Cuanto mayor sea el riesgo que el tratamiento de datos personales supone para los derechos y libertades de las personas físicas, más estrictas serán las obligaciones impuestas a los responsables del tratamiento de datos y más sólidas serán las garantías que deben establecerse.

El RGPD establece expresamente que los menores merecen una protección específica. Cuando los menores acceden a un servicio en línea, es obligatorio garantizar que se apliquen medidas específicas de protección de datos para asegurar un nivel adecuado de protección frente a los riesgos que plantea el uso que hacen del servicio. El Reglamento reconoce que es posible que los niños no sean plenamente conscientes de los riesgos y las consecuencias del uso que se hará de sus datos personales.

Principios pertinentes en materia de protección de datos

Las organizaciones que tratan datos están obligadas a respetar los principios de protección de datos, que son muy pertinentes para proteger a los menores en línea. Por ejemplo, el principio de minimización de datos exige a las organizaciones que reduzcan al mínimo la cantidad de datos de menores que se recogen y su uso posterior.

El principio de limitación de la finalidad exige que, cuando se recojan datos de menores para una finalidad concreta, la organización no los utilice para ninguna otra finalidad. El principio de integridad y confidencialidad exige que la organización adopte las medidas de seguridad adecuadas para proteger los datos de los menores frente a un uso ilícito o no autorizado.

Otra medida importante es la obligación de que las organizaciones que recogen y utilizan datos personales cumplan el principio de protección de datos desde el diseño y por defecto²³⁶. Esto exige que las medidas de protección de datos se integren en el servicio desde su diseño y que se utilicen por defecto los ajustes de privacidad más estrictos.

Estos requisitos también exigen que la organización adopte las medidas técnicas y organizativas adecuadas para proteger a los menores. El cumplimiento de este principio puede requerir diferentes medidas, en función del servicio ofrecido y del riesgo para el interesado. Dichas medidas podrían incluir lo siguiente:

- // garantizar que los datos personales de los niños no se compartan de forma sistemática con terceros;
- // garantizar que la identidad o la información de contacto de los niños no se pongan a disposición de terceros sin el consentimiento parental;
- // desactivar la geolocalización por defecto;
- // evitar las técnicas de «nudging» que animen o incentiven a los niños a facilitar información innecesaria.

El RGPD también establece requisitos específicos de transparencia para los menores. Exige que, cuando los niños utilicen un producto o servicio que trate sus datos personales (por ejemplo, si tienen una cuenta en un servicio concreto), se les proporcionen explicaciones fácilmente accesibles, en un lenguaje claro y sencillo, sobre cómo se utilizarán sus datos personales.

Esto es especialmente importante, ya que algunos niños no son conscientes de lo que se entiende por datos personales (por ejemplo, fotografías y vídeos) ni de que sus datos pueden utilizarse con fines como la personalización de anuncios y las experiencias en aplicaciones.

Base jurídica

Una característica fundamental del RGPD en materia de seguridad es que la organización que trata datos personales (el responsable del tratamiento) debe tener una base jurídica para hacerlo. Debe basarse en una de las seis bases jurídicas establecidas en el RGPD²³⁷. No existe una jerarquía en lo que respecta a las seis bases jurídicas previstas. Los responsables del tratamiento deben elegir la base más adecuada, teniendo en cuenta los requisitos de cada una de ellas.

Una de estas bases jurídicas es el consentimiento. El consentimiento debe darse de forma libre, específica, informada e inequívoca y expresarse mediante una clara acción afirmativa y las personas deben poder retirarlo con la misma facilidad con la que lo otorgaron²³⁸. El consentimiento no puede darse de forma libre si los menores no tienen una opción real o se sienten obligados a darlo. Para que el consentimiento sea informado, el responsable del tratamiento debe explicar, en un lenguaje claro y sencillo accesible para los niños, cómo pretende tratar los datos que recopila²³⁹.

Cuando un «servicio de la sociedad de la información»^f (como las plataformas de medios sociales y los videojuegos) se basa en el consentimiento como fundamento jurídico, los niños pueden dar su consentimiento para el tratamiento de sus datos personales a partir de los 16 años.

f. La mayoría de los servicios en línea se consideran un servicio de la sociedad de la información. Entre ellos figuran las aplicaciones, los motores de búsqueda, las plataformas de medios sociales, los servicios de mensajería en línea o los servicios de telefonía de voz por internet, los mercados en línea, los servicios de emisión en continuo de contenidos (por ejemplo, servicios de vídeo, música o juegos), los sitios web de noticias o educativos y cualquier sitio web que ofrezca otros bienes o servicios a los usuarios a través de internet. Véase: artículo 4, apartado 25, del RGPD.

El RGPD ofrece a los Estados miembros la posibilidad de reducir esta edad a cualquier edad comprendida entre los 13 y los 16 años. Si el niño es menor de 16 años, el tratamiento será lícito si el consentimiento lo da o autoriza el titular de la responsabilidad parental.

Los Estados miembros han establecido diferentes tramos de edad cuando los servicios de la sociedad de la información se basan en el consentimiento. Según las cifras disponibles a finales de 2025, 7 Estados miembros han fijado en 13 años la edad mínima para el consentimiento, 6 Estados miembros en 14 años, 5 Estados miembros en 15 años y 9 Estados miembros en 16 años.

De conformidad con el principio de responsabilidad proactiva, el responsable del tratamiento debe poder demostrar que ha cumplido el RGPD. Esto incluye garantizar que el consentimiento obtenido sea válido. No obstante, en la práctica, puede resultar difícil para un responsable del tratamiento garantizar que el consentimiento obtenido por el titular de la responsabilidad parental, en su caso, sea válido. Puede resultar difícil validar que la persona que da el consentimiento en nombre del menor tenga la autoridad legal para hacerlo.

Además, de conformidad con el principio de minimización de datos, un responsable del tratamiento solo debe tratar los datos necesarios para este fin y debe evitar el tratamiento de datos personales sensibles (como documentos que indiquen disposiciones de cuidados sensibles) para demostrar adecuadamente la validez del consentimiento.

Sin embargo, el requisito de obtener el consentimiento del titular de la responsabilidad parental no se aplica cuando los datos se tratan con arreglo a otra base jurídica, como un contrato o un interés legítimo (véase más adelante). Esto significa que, cuando una empresa de medios sociales se basa en uno de estos fundamentos para tratar los datos de los menores (por ejemplo, con el fin de crear su cuenta para acceder al servicio y sus interacciones en el servicio), no se aplican las garantías adicionales que conlleva el tratamiento de los datos de los menores basado en el consentimiento.

Cuando una organización trata datos personales en virtud de un contrato, corresponde a cada Estado miembro fijar la edad a partir de la cual un menor puede celebrar un contrato.

Otro fundamento en el que se basan los servicios en línea es el interés legítimo. Se refiere al tratamiento de datos personales de un menor para la satisfacción de los intereses legítimos del responsable del tratamiento o de un tercero, salvo que prevalezcan los intereses o los derechos y libertades fundamentales de la persona. El interés legítimo no es un fundamento jurídico «por defecto» para el tratamiento.

Cuando los responsables del tratamiento se basen en el interés legítimo para tratar datos personales de menores en virtud del RGPD, de conformidad con el principio de responsabilidad proactiva, deben garantizar que cumplen todos los requisitos del artículo 6, apartado 1, letra f), del RGPD antes de llevar a cabo el tratamiento⁹. Uno de estos requisitos es que los intereses legítimos del responsable del tratamiento no deben prevalecer sobre los intereses o los derechos y libertades fundamentales del niño²⁴⁰.

El TJUE ha señalado que, cuando un responsable del tratamiento lleva a cabo dicha evaluación, es necesario prestar especial atención a los casos en los que el interesado sea un niño. Ha señalado que, de conformidad con el considerando 38 del RGPD, los menores merecen una protección especial. Además,

⁹. Como ha confirmado el TJUE, el artículo 6, apartado 1, letra f), del RGPD impone tres condiciones acumulativas para que el tratamiento sea lícito: «en primer lugar, que el responsable del tratamiento o el tercero persigan un interés legítimo; en segundo lugar, que el tratamiento de los datos personales sea necesario para la satisfacción de ese interés legítimo, y, en tercer lugar, que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado». Véase: asunto C-252/21, Meta/Bundeskartellamt (ECLI:EU:C:2023:537), apartado 106.

el TJUE ha declarado que dicha protección específica debe aplicarse al tratamiento de datos personales de menores con fines de comercialización, creación de perfiles de personalidad o de usuario u oferta de servicios dirigidos directamente a los niños²⁴¹.

Los responsables del tratamiento también deben tener en cuenta el alcance y la intensidad de cualquier injerencia en los derechos y libertades del niño. Deben poder demostrar que se ha tenido en cuenta el interés superior del menor como consideración primordial y que se han aplicado las salvaguardias adecuadas²⁴². El interés superior del menor debe ser una consideración primordial a la hora de sopesar intereses contrapuestos.

Los responsables del tratamiento también deben tener en cuenta las expectativas razonables del menor en cuanto al uso que se hará de sus datos personales. Las expectativas del menor también pueden variar en función de su edad²⁴³. Dependiendo de la complejidad del tratamiento, la limitada capacidad del menor para comprender el tratamiento de datos aumenta el riesgo de que se produzcan consecuencias inesperadas o desproporcionadas del mismo.

Cabe señalar que el Comité Europeo de Protección de Datos (CEPD) considera que determinados tipos de operaciones de tratamiento de datos, como la elaboración de perfiles exhaustivos y las actividades de publicidad personalizada²⁴⁴, salvo en determinadas excepciones limitadas, no suelen ajustarse a la obligación de garantizar la protección específica de los niños²⁴⁵.

Cuando los intereses legítimos del responsable del tratamiento entren en conflicto con los intereses o los derechos y libertades fundamentales de un menor, los intereses y derechos de este último deben prevalecer, por regla general. Cuando esto no sea posible, el responsable del tratamiento deberá basarse en otro fundamento jurídico para tratar los datos o dejar de tratarlos.

Otras disposiciones pertinentes

El RGPD también ofrece una mayor protección a los menores en relación con el derecho de supresión, teniendo en cuenta que es posible que el menor no haya sido plenamente consciente de los riesgos que conlleva el tratamiento y, posteriormente, desee suprimir dichos datos²⁴⁶. Asimismo, establece que los menores no deben ser objeto de elaboración de perfiles ni de toma de decisiones automatizadas²⁴⁷ y ofrece protecciones específicas para los menores en lo que respecta a la comercialización dirigida a ellos²⁴⁸.

El Comité Europeo de Protección de Datos (CEPD) ha sostenido que «las organizaciones deben, en general, evitar la elaboración de perfiles de menores con fines de comercialización [...] y que dicha elaboración de perfiles debe permitirse en circunstancias muy limitadas, como cuando sea necesario para proteger el bienestar del menor»²⁴⁹.

El RGPD también establece las circunstancias en las que se requiere una evaluación de impacto relativa a la protección de datos (EIPD). Esto exige que las organizaciones evalúen los riesgos asociados al tratamiento propuesto de los datos personales de los usuarios y, en caso necesario, reduzcan el riesgo que supone para los usuarios, incluidos los niños. Las evaluaciones de riesgos deben tener en cuenta las diferentes edades y necesidades de desarrollo de los usuarios menores de edad.

Las evaluaciones de riesgos para los niños también deben tener en cuenta los riesgos que el tratamiento de sus datos personales puede suponer para su bienestar general. Esto incluye cualquier perjuicio físico, mental o económico al que puedan verse expuestos como consecuencia del tratamiento. El principio del interés superior del menor debe ser una de las principales herramientas de evaluación de riesgos a la hora de llevar a cabo una EIPD relativa al tratamiento de los datos personales de los menores.

Cuando el riesgo siga siendo elevado tras la aplicación de las medidas propuestas, la organización está obligada a consultar a su autoridad de protección de datos (APD). La APD está obligada a proporcionar asesoramiento por escrito y también puede hacer uso de cualquiera de sus facultades, incluida la prohibición del tratamiento cuando los riesgos sean demasiado elevados y no puedan mitigarse adecuadamente²⁵⁰.

REGLAMENTO DE INTELIGENCIA ARTIFICIAL (REGLAMENTO DE IA)

Además del Reglamento de Servicios Digitales, el Reglamento de Inteligencia Artificial (Reglamento de IA) establece un marco jurídico exhaustivo para la regulación de la inteligencia artificial (IA) en la UE. El Reglamento de IA desempeña un papel importante en el refuerzo de la protección de los derechos de los niños al imponer salvaguardias para proteger la salud, la seguridad y los derechos fundamentales durante el desarrollo y la implantación de la IA. El Reglamento de IA sigue un enfoque basado en el riesgo e introduce normas para los sistemas de IA en función del posible nivel de riesgo que puedan suponer.

Varios casos de uso de la IA con un impacto significativo en los derechos de los niños se clasifican como de alto riesgo en virtud del Reglamento de IA, por ejemplo, cuando se utiliza en el ámbito de la educación y la formación profesional. Los sistemas de IA de alto riesgo deben cumplir determinados requisitos para garantizar su seguridad y fiabilidad, como la gestión de riesgos, la transparencia y la supervisión humana. En particular, el sistema de gestión de riesgos de un sistema de IA de alto riesgo debe tener en cuenta si existe una probabilidad de que se produzcan efectos adversos en personas menores de 18 años.

A la hora de evaluar el impacto sobre los derechos fundamentales del uso concreto de un sistema de IA de alto riesgo^h, algunos responsables de la implantación de dichos sistemas deben tener en cuenta las categorías de personas y grupos que es probable que se vean afectados por el uso del sistema, entre los que pueden figurar los menores. La Comisión Europea ha publicado para consulta pública un proyecto de directrices sobre la clasificación de los sistemas de IA de alto riesgo, que incluye ejemplos de prácticas que entran en el ámbito de aplicación del Reglamento de IA o quedan fuera de él²⁵¹.

Además, debido a la naturaleza cambiante de los sistemas de IA, los legisladores han acordado rápidamente el Ómnibus Digital sobre IA para reforzar aún más las normas que también contribuyen a una mejor protección de los menores. En particular, las nuevas normas prohíben los sistemas de IA que generan contenidos no consentidos, sexualmente explícitos e íntimos o material de abuso sexual de menores, como las aplicaciones de «nudificación» basadas en IA. Las obligaciones para los sistemas de IA de alto riesgo, tal como se acordó en el Ómnibus Digital sobre IA, empezarán a aplicarse en diciembre de 2027 (en el caso de los sistemas de IA independientes, como determinados sistemas de IA en el ámbito educativo) y en agosto de 2028 (en el caso de los sistemas de IA integrados en productos regulados, como los juguetes).

Prácticas prohibidas

El Reglamento de IA prohíbe las prácticas de IA que manipulen, engañen o aprovechen las vulnerabilidades de los menores. Estas prohibiciones tienen por objeto evitar que los sistemas de IA manipulen a los menores o aprovechen las limitaciones cognitivas y de otro tipo que estos puedan tener a la hora de

h. Las obligaciones para los sistemas de IA de alto riesgo, tal como se acordó en el Ómnibus Digital sobre IA, empezarán a aplicarse en diciembre de 2027 (en el caso de los sistemas de IA independientes, como determinados sistemas de IA en el ámbito educativo) y en agosto de 2028 (en el caso de los sistemas de IA integrados en productos regulados, por ejemplo, juguetes).

tomar decisiones que, de otro modo, no habrían tomado, así como protegerlos de influencias indebidas y perjudiciales, de la manipulación y de la explotación.

Estas disposiciones empezaron a aplicarse el 2 de febrero de 2025. La Comisión ha publicado directrices sobre las prácticas de IA prohibidas, que incluyen ejemplos de prácticas que entran en el ámbito de aplicación del Reglamento de IA o quedan fuera de él²⁵².

Un ejemplo de práctica de IA prohibida es una aplicación basada en la IA que anime a los menores a completar retos cada vez más arriesgados, como trepar por muebles, explorar estanterías altas o manipular objetos afilados, a cambio de recompensas digitales y elogios virtuales. Estos sistemas aprovechan las vulnerabilidades de los menores abusando de su curiosidad natural y su deseo de recompensas, y pueden causarles un perjuicio significativo.

Otro ejemplo de práctica de IA prohibida son los juegos diseñados para ser altamente adictivos, aprovechando las vulnerabilidades inherentes a los niños y adolescentes (incluida la falta de autocontrol). Estos juegos utilizan la IA para analizar el comportamiento y las preferencias individuales de los niños, sobre cuya base crean recompensas personalizadas e impredecibles mediante programas de refuerzo adictivos y bucles similares a los de la dopamina. Esto fomenta el juego excesivo y el uso compulsivo.

Estos juegos están diseñados para ser (o tener el efecto de ser) altamente adictivos, aprovechando las vulnerabilidades inherentes a los niños. Esto incluye su capacidad limitada para comprender las consecuencias a largo plazo, su susceptibilidad a la presión, la falta de autocontrol y su inclinación hacia la gratificación instantánea.

Modelos de IA de uso general

Para los modelos de IA de uso general de mayor rendimiento que entrañan un riesgo sistémico, el Reglamento de IA impone obligaciones específicas de evaluación y mitigación de riesgos. Para cumplir estas normas, la mayoría de los principales proveedores de modelos de IA de uso general han firmado el Código de buenas prácticas para la IA de uso general²⁵³.

Los proveedores de IA de uso general deben evaluar y mitigar escenarios de riesgo concretos. Esto puede incluir la difusión de riesgos de difusión de contenidos ilícitos, falsos o discriminatorios, así como los riesgos derivados de contenidos ilícitos, violentos, que inciten al odio, radicalizantes o falsos, y la notificación de los resultados de este proceso de gestión de riesgos a la Comisión Europea antes de la comercialización.

Parte de las medidas de mitigación que deben adoptar los proveedores de modelos de IA de uso general consisten en supervisar y filtrar las entradas del modelo. Esto incluye la prevención de la generación de contenidos nocivos. Las obligaciones relativas a los modelos de IA de uso general empezaron a aplicarse el 2 de agosto de 2025.

Obligaciones de transparencia

A fin de ayudar a evitar el fraude, la suplantación de identidad y el engaño, el Reglamento de IA impone obligaciones de transparencia a los proveedores y responsables del despliegue de determinados sistemas de IA²⁵⁴. En virtud del Reglamento de IA, los proveedores deben garantizar que los sistemas de IA destinados a interactuar directamente con las personas (como los chatbots) se diseñen y desarrollen de manera que las personas afectadas estén informadas de que están interactuando con un sistema de IA,

a menos que esto sea evidente. Esta obligación se aplica en cualquier caso a los chatbots que interactúan con niños.

La divulgación de información no aborda por completo los riesgos de dependencia emocional. Sin embargo, el carácter interactivo y a menudo atractivo de estos sistemas hace que sea fundamental que se informe explícitamente a los usuarios de que están interactuando con un sistema de IA, programado para potenciar su interacción, y no con una persona.

Sistemas de IA generativa

Los proveedores y responsables del despliegue de sistemas de IA generativa tienen la obligación de señalar y permitir la detección cuando los contenidos, como imágenes, audio o vídeo, se hayan generado o manipulado artificialmente, así como de etiquetar las ultrafalsificaciones y determinadas publicaciones generadas por IA sobre asuntos de interés público.

Los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica deben informar a las personas expuestas al funcionamiento del sistema. La Comisión Europea facilita el cumplimiento de estas obligaciones mediante, entre otras cosas, la publicación de un Código de buenas prácticas sobre el marcado y el etiquetado de los contenidos generados por IA²⁵⁵, así como de unas directrices que se están preparando actualmente tras haber sido publicadas para consulta pública²⁵⁶. Las obligaciones relativas a los requisitos de transparencia se aplicarán a partir del 2 de agosto de 2026.

Asistentes de IA

Los asistentes de IA están ganando cada vez más popularidad entre los niños y se han detectado determinados riesgos asociados a su uso. En virtud del Reglamento, la clasificación de los asistentes de IA y los chatbots similares depende principalmente de su finalidad prevista, su funcionalidad y su contexto de uso.

En función de estos factores, un asistente de IA podría constituir una práctica prohibida (por ejemplo, en casos en los que se aprovechen las vulnerabilidades de los niños de formas significativamente perjudiciales). También podrían considerarse sistemas de IA de alto riesgo (por ejemplo, cuando incorporan funcionalidades de reconocimiento de emociones o en determinados casos de uso en el contexto educativo). Por último, pueden estar sujetos a obligaciones de transparencia que exijan que se informe a los usuarios de que no están interactuando con una persona.

INSTRUMENTOS DE PROTECCIÓN DE LOS CONSUMIDORES

A la hora de abordar los daños a los que se enfrentan los niños en el entorno digital, es importante tener en cuenta los enfoques de responsabilidad penal y de responsabilidad civil y por los daños causados por productos defectuosos.

La responsabilidad penal podría abordar la prohibición y el castigo de conductas perjudiciales específicas, como la distribución de material de abuso sexual de menores o la captación sexual en línea, y se basa en el enjuiciamiento por parte del Estado y en sanciones penales. Si bien es indispensable para los delitos más graves, el enjuiciamiento de infracciones penales es principalmente reactivo. Normalmente tiene lugar después de que se haya producido el daño, identifica y se centra en los infractores individuales, en

lugar de en las condiciones sistémicas que permiten que se produzca el daño. Sin embargo, la tipificación de determinadas conductas también incluye importantes elementos preventivos y anticipatorios.

Por otra parte, un enfoque de responsabilidad civil y por los daños causados por productos defectuosos podría proporcionar medidas preventivas y compensatorias entre distintas partes privadas. Se centra en la asignación de derechos, obligaciones y responsabilidades entre las partes privadas, incluidas las empresas que diseñan y gestionan medios sociales y otros servicios digitales, y en ofrecer vías de recurso en caso de incumplimiento de dichas obligaciones.

La legislación en materia de protección de los consumidores desempeña un papel clave en los asuntos de responsabilidad civil y por los daños causados por productos defectuosos. Es importante señalar que esta perspectiva permite a los reguladores y a los litigantes privados impugnar las decisiones de diseño de los proveedores de servicios en línea. Es precisamente esta perspectiva de la responsabilidad por los daños causados por productos defectuosos la que ha impulsado los avances jurídicos recientes más trascendentales en los Estados Unidos.

«Las plataformas deben crecer con el niño. [...] Cualquier sistema de recomendación dirigido a un menor debe estar optimizado para su bienestar, no para fomentar la interacción.»

— GABRIELE BATTIMELLI,
EMBAJADOR DE ITALIA PARA «UNA
INTERNET MEJOR PARA LOS NIÑOS»

En los Estados Unidos, uno de los casos recientes sobre diseños adictivos en las plataformas se basa en la legislación en materia de protección de los consumidores. Un jurado de Nuevo México dictaminó en marzo de 2026 que Meta, como operador de sus plataformas en línea, infringió deliberadamente la legislación en materia de protección de los consumidores y condenó a la empresa a pagar 375 millones USD.

El asunto fue presentado por el fiscal general del Estado en virtud de la legislación sobre prácticas desleales y se centró en el diseño de las plataformas y las prácticas de seguridad, incluidos los sistemas de recomendación que exponían a los menores a depredadores. El jurado determinó que la empresa había engañado a los consumidores sobre la seguridad de sus servicios, mientras que los documentos internos demostraban que era consciente del daño causado.

Paralelamente, en Los Ángeles, el primer juicio pionero por «adicción a los medios sociales» concluyó con un veredicto del jurado en contra de Meta y YouTube por una serie de acusaciones, entre las que se incluían el diseño negligente y la falta de advertencias. El asunto se basa en el Derecho privado de responsabilidad civil. El órgano jurisdiccional identificó explícitamente características, como el desplazamiento infinito por la pantalla, las fuentes algorítmicas, la reproducción automática y los mecanismos de maximización de la interacción, como factores que contribuían al daño sufrido por los menores. La sentencia reconoce que las características de diseño que favorecen la adicción pueden constituir defectos del producto susceptibles de recurso, en particular cuando las empresas son conscientes de los riesgos y no los mitigan.

En la UE, la legislación en materia de protección de los consumidores se aplica a los niños como categoría de consumidores vulnerables a través de varios instrumentos. Actúa como una «red de seguridad» hori-

zontal que se aplica a todos los comerciantes, bienes o servicios dirigidos a los consumidores, también en el entorno digital, independientemente del modelo de negocio o de las tecnologías utilizadas.

Las normas vigentes de la UE en materia de protección de los consumidores, en particular la Directiva sobre las prácticas comerciales desleales (DPCD), reconocen a los niños como consumidores vulnerables que requieren una mayor protección. La DPCD prohíbe las prácticas comerciales engañosas y agresivas que explotan la credulidad o la falta de experiencia de los niños.

También prohíbe que se exhorte a los niños para que compren o convenzan a sus progenitores de que les compren los productos anunciados. Tal como se explica en las directrices sobre la DPCD²⁵⁷, los patrones oscuros, las funciones destinadas a maximizar el gasto o la atención (por ejemplo, las monedas poco claras integradas en las aplicaciones) o la comercialización desleal por parte de influyentes también pueden constituir prácticas comerciales desleales. A pesar de ello, el control de adecuación de la equidad digital²⁵⁸ constató que los consumidores en general, y los niños y adolescentes en particular, necesitan una mayor protección en línea.

La Directiva sobre los derechos de los consumidores (DDC) impone obligaciones precontractuales, por ejemplo, la transparencia sobre la fijación de precios, la identidad del comerciante o el derecho de desistimiento. Aunque no se refiere específicamente a los niños, se aplica a todas las transacciones digitales (por ejemplo, la compra de monedas virtuales en los videojuegos), incluidas aquellas en las que participan menores.

Además, la Directiva sobre cláusulas contractuales abusivas (DCCA) considera abusivas y no vinculantes las cláusulas contractuales no negociadas individualmente si crean un desequilibrio importante en detrimento del consumidor. Esto incluye los casos en que el consumidor es menor de edad.

Por último, el Reglamento sobre la seguridad general de los productos exige que todos los productos de consumo que entran en su ámbito de aplicación, incluidos los productos conectados, sean seguros. El ámbito de aplicación de este Reglamento es amplio, de modo que puede actuar como red de seguridad para todos los productos introducidos o comercializados en el mercado de la UE.

A la hora de evaluar la seguridad de los productos, los fabricantes deben tener en cuenta las categorías de consumidores que utilizan el producto, verificando el riesgo para los consumidores vulnerables, como los niños. Asimismo, deben adoptar las medidas de mitigación de riesgos correspondientes. El Reglamento se centra en la protección de la salud física y mental de los consumidores, lo que puede ser pertinente, por ejemplo, para las aplicaciones o los chatbots populares entre los menores.

DIRECTIVA SOBRE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS

La Directiva sobre responsabilidad por los daños causados por productos defectuosos es un marco armonizado de responsabilidad civil que garantiza que las víctimas de productos defectuosos puedan reclamar una indemnización al fabricante en caso de daño. La nueva Directiva sobre responsabilidad por los daños causados por productos defectuosos entró en vigor el 8 de diciembre de 2024 y los Estados miembros deben transponerla a más tardar el 9 de diciembre de 2026.

La Directiva revisada mantiene intactos los fundamentos de la Directiva original. Corresponde a la víctima demostrar que un producto es defectuoso y que existe un nexo causal entre el carácter defectuoso y el daño concreto sufrido. La Directiva revisada sobre responsabilidad por los daños causados por productos

defectuosos aclara el ámbito de aplicación para abarcar los programas informáticos, incluidas las aplicaciones, los sistemas operativos y los sistemas de IA y especifica las normas de responsabilidad en caso de que se produzca una modificación sustancial de los productos que les confiera una «segunda vida».

También aclara que los daños indemnizables en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos pueden incluir daños mentales reconocidos médicamente. La Directiva también adapta las normas en materia de responsabilidad a unas cadenas de valor mundiales cada vez más complejas, garantizando que pueda identificarse al menos a un operador económico responsable establecido en la UE (incluidas, potencialmente, las plataformas).

La nueva Directiva establece una vía de indemnización en los casos en que los productos digitales defectuosos causen daños a los niños. Por ejemplo, un niño que desarrolle depresión debido al diseño adictivo de una aplicación, o que se autolesione a raíz de las respuestas peligrosas de un chatbot, puede ahora tener derecho a una indemnización en virtud de la Directiva sobre responsabilidad por los daños causados por productos defectuosos.

DIRECTIVA DE SERVICIOS DE COMUNICACIÓN AUDIOVISUAL

La Directiva de Servicios de Comunicación Audiovisual es la pieza central de la legislación de la UE en materia de medios de comunicación que regula los contenidos audiovisuales. Establece obligaciones sectoriales específicas para los servicios de comunicación audiovisual y las plataformas de intercambio de vídeos con el fin de proteger a los menores frente a contenidos audiovisuales nocivos.

En virtud de dicha Directiva, las plataformas de intercambio de vídeos deben incluir en sus condiciones generales las normas en materia de contenidos mediáticos de la UE. Esto incluye las destinadas a proteger a los menores de contenidos que puedan perjudicar su desarrollo físico, mental o moral. También están obligadas a adoptar las medidas adecuadas (por ejemplo, mecanismos para denunciar o señalar contenidos nocivos, verificación de la edad, controles parentales y sistemas de clasificación de contenidos) para impedir que los menores vean contenidos audiovisuales nocivos. Los contenidos más nocivos, como la pornografía o la violencia gratuita, deben estar sujetos a las medidas más estrictas para impedir que los menores vean contenidos nocivos.

La evaluación en curso y la próxima revisión de la Directiva de Servicios de Comunicación Audiovisual, prevista para el tercer trimestre de 2026, se centrarán especialmente en la protección de los menores como espectadores vulnerables en línea. Se estudiará la pertinencia de las normas actuales y se determinarán las posibles deficiencias de la legislación vigente. Esto incluirá evaluar si debe hacerse más para garantizar que los espectadores, sobre todo los menores, estén adecuadamente protegidos cuando vean contenidos audiovisuales en línea. Esto incluye los contenidos puestos a disposición por los influencers, teniendo en cuenta la evolución del mercado y de la normativa. Esta evolución y los cambios en los hábitos de consumo audiovisual generan problemas que pueden poner en peligro a los espectadores, en particular a los menores.

Han surgido nuevas amenazas y riesgos en el entorno en línea que han dado lugar a una mayor exposición de los menores a contenidos audiovisuales nocivos, como el ciberacoso, los trastornos alimentarios y la incitación al suicidio o a las autolesiones. La revisión analizará si es necesario precisar más el concepto de «contenido audiovisual nocivo» y qué medidas son necesarias para garantizar que los menores no vean dicho contenido.

REGLAMENTO SOBRE LA PUBLICIDAD POLÍTICA

El Reglamento sobre la publicidad política establece obligaciones de transparencia y diligencia debida para la prestación de servicios de publicidad política. El Reglamento introduce requisitos específicos para el uso de técnicas de segmentación y de entrega de anuncios en la publicidad política en línea que se basan en el tratamiento de datos personales. El Reglamento fomenta la protección de los menores, al tiempo que garantiza la igualdad de condiciones para quienes votan por primera vez.

Por una parte, el Reglamento prohíbe el uso de la elaboración de perfiles que implique el tratamiento de datos personales de menores de los que se sepa que están al menos un año por debajo de la edad electoral nacional. Por otra parte, el Reglamento permite que la publicidad política transparente llegue a quienes votan por primera vez, lo que les permite ejercer sus decisiones democráticas con conocimiento de causa.

PROTECCIÓN CONTRA EL ABUSO Y LA EXPLOTACIÓN SEXUALES DE MENORES EN LÍNEA

El abuso y la explotación sexuales de menores en línea se encuentran entre los riesgos más graves a los que pueden enfrentarse los niños y adolescentes en el mundo digital. Los autores son adultos, pero también otros menores. Es necesario informar a los niños y adolescentes sobre los riesgos, incluido el sexteo y la sextorsión, así como sobre las posibles consecuencias jurídicas para los autores.

Las víctimas explotadas por familiares y cuidadores suelen necesitar medidas de protección infantil basadas en el Derecho civil, junto con asistencia social y una acogida segura. Muchas víctimas pueden necesitar psicoterapia.

Las medidas de protección de los menores contra el abuso y la explotación sexuales de menores en línea forman parte de la dimensión penal de la protección infantil, que se sitúa en la intersección de las competencias de la UE y de los Estados miembros.

Al determinar que determinados contenidos son ilícitos, ya sea por sí mismos o por estar relacionados con una actividad ilegal, estos instrumentos también dan lugar a las disposiciones pertinentes en materia de diligencia debida previstas en el Reglamento de Servicios Digitales. Abordan la cuestión de los contenidos ilícitos que entran en el ámbito de aplicación y establecen un marco eficaz contra la difusión de dichos contenidos.

La Comisión Europea ha tomado medidas para prevenir y combatir el abuso sexual de menores en línea. En 2022, presentó una propuesta de marco regulador de la UE permanente y exhaustivo para prevenir y luchar contra el abuso sexual de menores. Este marco incluye obligaciones para los proveedores de servicios en línea con el fin de evitar la difusión de material de abuso sexual de menores y la captación sexual a través de sus servicios. Solo cuando las medidas de prevención no sean suficientes, los proveedores de servicios en línea podrían verse obligados a detectar, denunciar, eliminar o bloquear el abuso sexual de menores en línea.

Con arreglo a la propuesta, las autoridades nacionales competentes estarían facultadas para solicitar la emisión de órdenes de detección, eliminación o bloqueo por parte de autoridades judiciales o administrativas independientes. Dichas órdenes solo se emitirían tras una evaluación exhaustiva de su necesidad y proporcionalidad.

La propuesta también prevé la creación de un nuevo Centro de la UE sobre Abuso Sexual de Menores, con el fin de ayudar a los proveedores de servicios digitales y a las autoridades a cumplir sus obligaciones en virtud del Reglamento. Las negociaciones sobre el Reglamento siguen en curso. La Comisión Europea apoya al Parlamento Europeo y al Consejo en la consecución de un acuerdo que garantice la protección efectiva de los menores, respetando plenamente todos los derechos fundamentales afectados, así como la coherencia con la legislación vigente, en particular el Reglamento de Servicios Digitales.

Paralelamente, el reciente acuerdo de los colegisladores sobre la refundición de la Directiva sobre el abuso sexual de menores ha reforzado aún más el marco de la UE contra el abuso y la explotación sexuales de menores, tanto en línea como fuera de línea. Las normas revisadas actualizan el marco vigente para garantizar que nuevas amenazas, como el material de abuso sexual de menores generado por IA, la captación sexual y la sextorsión, así como la retransmisión en directo de abuso sexual de menores, se tipifiquen como delito y se persigan eficazmente.

Las normas revisadas también reforzarán el marco jurídico para prevenir el abuso sexual de menores y ayudar a las víctimas. Esto se logrará imponiendo controles de antecedentes personales a las personas que trabajen en contacto estrecho y directo con menores, o garantizando que las víctimas puedan solicitar el enjuiciamiento durante un período suficiente después de que se haya cometido el delito.

Además de las iniciativas legislativas, la UE también adopta medidas no legislativas, como la financiación y la facilitación de la coordinación y la cooperación. Por ejemplo, la Red de Prevención del Abuso Sexual de los Menores reúne a cincuenta expertos para intercambiar buenas prácticas, contribuir a la investigación y apoyar el desarrollo y la aplicación de medidas de prevención del abuso sexual de menores, también en línea, evaluadas rigurosamente.

El Derecho penal es necesario para luchar contra el abuso sexual de menores, pero no puede ser la única herramienta para abordar eficazmente este horrible delito. La protección de los menores frente al abuso y la explotación sexuales requiere un enfoque que implique a toda la sociedad. En él deben participar las autoridades públicas, las autoridades policiales, las autoridades judiciales, las instituciones educativas, las organizaciones de la sociedad civil, las familias, las comunidades y los proveedores de medios sociales y otros servicios digitales. La eficacia de la prevención y las respuestas a estos delitos no depende únicamente de medidas legislativas sólidas, sino también de esfuerzos coordinados y de una acción intersectorial multinivel.

PREVENCIÓN DE LA RADICALIZACIÓN

El Reglamento de la UE sobre la lucha contra la difusión de contenidos terroristas en línea protege a las poblaciones vulnerables, incluidos los niños, de la exposición a material radicalizador en línea. El Reglamento exige a los prestadores de servicios de alojamiento de datos que retiren los contenidos terroristas en el plazo de una hora a partir de la recepción de una orden de retirada emitida por una autoridad nacional competente.

Esto se complementa con varias iniciativas no legislativas. Una de estas medidas es el Foro de la UE sobre Internet. El Foro es una plataforma público-privada que reúne a los Estados miembros de la UE, las autoridades policiales, la industria y la sociedad civil para coordinar las respuestas contra los abusos. Esto incluye la explotación de plataformas en línea por parte de terroristas, extremistas violentos y otros agentes malintencionados, como los que captan a menores con fines de abuso sexual, tráfico de drogas, delincuencia organizada, trata de seres humanos o tráfico ilícito de migrantes.

Los menores de toda la UE sufren un grave riesgo de ser víctimas de delitos o de ser incitados para cometer delitos, tanto en línea como fuera de línea. La Comisión Europea está elaborando actualmente un plan de acción para la protección de los niños contra la delincuencia. Se espera que esto complemente los instrumentos existentes al detectar las lagunas que aún persisten y que proporcione un enfoque más coherente y coordinado para mejorar la protección de los niños frente a la delincuencia, tanto en calidad de víctimas como de autores, en línea y fuera de línea.

PLAN DE ACCIÓN CONTRA EL CIBERACOSO

El ciberacoso es un problema cada vez mayor para los niños y adolescentes en el mundo en línea, con importantes repercusiones en la salud mental y el bienestar, la participación y el desarrollo de los niños.

Para hacer frente a su preocupante prevalencia, en marzo de 2026 la Comisión Europea adoptó el Plan de Acción contra el Ciberacoso²⁵⁹. El Plan de Acción tiene por objeto prevenir el ciberacoso, facilitar su denuncia y garantizar un apoyo eficaz a las víctimas. En el marco del Plan de Acción, se anima a los Estados miembros de la UE a adoptar medidas complementarias a escala nacional.

Esto incluye el desarrollo de estrategias nacionales de lucha contra el acoso, el refuerzo de la prevención y la detección precoz en las escuelas y otros entornos en los que los niños pasan tiempo. La mejora de los servicios de apoyo a las víctimas y la garantía de que los sistemas de denuncia estén vinculados a un apoyo jurídico, social, psicológico y educativo adecuado son otros ámbitos de actuación importantes en el marco del Plan de Acción.

Además, la Recomendación de la Comisión sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia que redunden en el interés superior del menor²⁶⁰ invita a los Estados miembros de la UE a adoptar todas las medidas legislativas, administrativas, sociales y educativas adecuadas para prevenir el acoso, también en línea, y proteger a los niños frente a él. Esto incluye el desarrollo de planes integrales contra el acoso.

SOLUCIÓN DE LA UE PARA LA VERIFICACIÓN DE LA EDAD

Además de la legislación vigente, la Comisión Europea ha creado y está ampliando un conjunto de herramientas operativas para la verificación de la edad con el fin de proteger a los niños y adolescentes en línea y limitar su exposición a contenidos nocivos. Este conjunto de herramientas ofrece redes, plataformas, soluciones técnicas y canales para proteger y empoderar a los menores en línea.

La Comisión ha desarrollado una solución de verificación de la edad de la UE que es sólida, fácil de usar y preserva la privacidad. A tal fin, se ha puesto a disposición de los Estados miembros un plan director para su personalización y aplicación. Cuando se personaliza, puede tener en cuenta diferentes tramos de edad. Los Estados miembros pueden publicar la solución como aplicación independiente o integrarla como funcionalidad de verificación de la edad en sus carteras de identidad digital de la UE. La solución es de código abierto, por lo que los terceros países o los agentes del mercado también pueden adoptarla y seguir desarrollándola.

La solución de la UE para la verificación de la edad podría ser una herramienta adecuada para aplicar restricciones de edad en la práctica, siempre que vaya acompañada de opciones adecuadas para que los menores demuestren su edad. Los Estados miembros de la UE aplican enfoques diversos en cuanto al uso y la expedición de documentos de identidad o identificaciones electrónicas y es posible que no todos los menores dispongan de su propio pasaporte. Por ello, la designación de proveedores de prueba

de la edad de confianza, capaces de expedir pruebas de edad para la edad requerida, es esencial para el funcionamiento eficaz de la verificación de la edad en la UE.

Para acelerar este proceso, la Comisión Europea publicó una Recomendación sobre el establecimiento de un marco común para las tecnologías de verificación de la edad a escala de la UE. Como parte de la Recomendación, la Comisión está definiendo un Sistema de Verificación de la Edad de la UE en cooperación con los Estados miembros. El Sistema detallará los requisitos relativos al modelo de confianza, la gobernanza y los requisitos que deben cumplir los proveedores de declaraciones de prueba de la edad y de soluciones de verificación de la edad.

La Recomendación anima a los Estados miembros de la UE a hacer uso del plan director de verificación de la edad de la UE, adaptarlo a sus contextos nacionales y poner a disposición soluciones de verificación de la edad a más tardar el 31 de diciembre de 2026 sobre la base del plan.

Además, se invitó a los Estados miembros a presentar un plan de aplicación a la Comisión a más tardar el 30 de junio de 2026 en el que se describa cómo tienen previsto poner a disposición una solución de verificación de la edad de la UE. Se anima a los Estados miembros a colaborar entre sí y a cooperar con la Comisión Europea, los investigadores y la sociedad civil en la implantación de sus soluciones nacionales. Los retos que plantea la verificación de la edad, incluidos los posibles riesgos de fragmentación normativa en toda la UE, se analizan más adelante en este capítulo, en la sección «Asuntos pendientes».

Resultados de la aplicación actual

La eficacia de la legislación vigente de la UE depende de su aplicación. El Reglamento de Servicios Digitales introdujo una arquitectura de aplicación fundamentalmente nueva, centralizada en la Comisión para las plataformas más grandes y combinada con la aplicación a escala nacional a través de los coordinadores de servicios digitales. Esta arquitectura ahora está dando lugar a decisiones, procedimientos y cambios tangibles en materia de cumplimiento y empieza a perfilarse un historial de resultados.

El Reglamento de IA opta por una estructura de aplicación adaptada de manera similar, con una aplicación centralizada en la Comisión para los modelos de IA de uso general y la mayoría de los sistemas de IA basados en modelos de IA de uso general cuando el proveedor del sistema y el modelo de IA es el mismo (o pertenece a la misma empresa). El Reglamento omnibus digital sobre IA introduce una innovación adicional, ya que la aplicación relacionada con los sistemas de IA designados o integrados en plataformas en línea de muy gran tamaño o en motores de búsqueda en línea de muy gran tamaño en virtud del Reglamento de Servicios Digitales también se centraliza en la Comisión.

El RGPD es aplicado por autoridades nacionales independientes de protección de datos (APD). Siguen adoptando decisiones, imponiendo multas sustanciales y otras medidas correctoras cuando determinan que los responsables del tratamiento han infringido las normas de protección de datos.

La aplicación de la Directiva de Servicios de Comunicación Audiovisual corre a cargo de las autoridades y organismos reguladores nacionales. La Directiva de Servicios de Comunicación Audiovisual introdujo requisitos para garantizar la independencia institucional y funcional de las autoridades y organismos reguladores nacionales, que se han visto reforzados por el Reglamento Europeo sobre la Libertad de los Medios de Comunicación.

La aplicación de la legislación en materia de protección de los consumidores, incluidas las normas derivadas de las Directivas y Reglamentos de la UE, es principalmente competencia de las autoridades

y los órganos jurisdiccionales de los Estados miembros. Si bien la Comisión no dispone actualmente de competencias de ejecución directas en el ámbito de la legislación en materia de protección de los consumidores, coordina y apoya la labor de ejecución de los Estados miembros en virtud del Reglamento sobre la cooperación en materia de protección de los consumidores (CPC). Esto establece un marco de cooperación transfronteriza en materia de ejecución para que las autoridades CPC de los Estados miembros aborden conjuntamente las infracciones transfronterizas y a escala de la UE de la legislación en materia de protección de los consumidores.

ESTRUCTURA DE APLICACIÓN DEL REGLAMENTO

DE SERVICIOS DIGITALES

La estructura de aplicación del Reglamento de Servicios Digitales implica una competencia directa y centralizada de la Comisión en lo que respecta a las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño, así como la coordinación y la cooperación con varias autoridades nacionales, en particular en el contexto de la Junta Europea de Servicios Digitales, que también cuenta con un grupo de trabajo específico sobre la protección de los menores.

Se trata de un nuevo marco de aplicación que tiene la ventaja de centralizar la aplicación a nivel de la Comisión para las plataformas más grandes, que operan sin trabas a través de las fronteras. Algunas de estas plataformas se encuentran entre las empresas más grandes y con mayores recursos del mundo, con ingresos que a menudo superan el PIB de los Estados miembros de la UE. Este marco también promueve una aplicación coherente de las normas en toda la UE y hasta el nivel nacional (por ejemplo, a través de las directrices sobre la protección de los menores y la jurisprudencia).

El efecto disuasorio es considerable, ya que cuenta con una de las mayores competencias para imponer multas del mundo y con medidas provisionales que pueden dar lugar a un cambio rápido en las prácticas de las plataformas, como demuestran los compromisos asumidos por TikTok y la retirada de TikTok Lite en la UE²⁶¹. En el contexto de las investigaciones, la Comisión Europea dispone de sólidas herramientas de ejecución y competencias de investigación. En particular, esto incluye la capacidad de solicitar datos e información detallados y sensibles, así como de llevar a cabo inspecciones en las instalaciones de los proveedores. Esto permite un acceso sin precedentes a los sistemas, el diseño y las decisiones de los proveedores.

En casos extremos en los que la infracción persista y cause daños graves y urgentes, la Comisión puede solicitar al coordinador de servicios digitales del Estado miembro de establecimiento del proveedor que pida a la autoridad judicial competente que ordene la restricción temporal del acceso al servicio²⁶².

Las medidas de ejecución adoptadas por la Comisión Europea han requerido un importante esfuerzo de desarrollo de capacidades y ahora se están acelerando cada vez más. Poco a poco, se están volviendo más rápidas, como demuestran las conclusiones preliminares sobre TikTok en relación con el diseño potencialmente adictivo y sobre Meta en relación con la garantía de edad. Los indicadores de cumplimiento establecidos en las directrices sobre la protección de los menores han contribuido a este fin.

La descripción inicial de las expectativas de la Comisión sobre cuestiones clave en las medidas de ejecución, incluidas las conclusiones preliminares y los compromisos, también debe servir de referencia y reflejarse en la práctica continua de los ciclos de evaluación y mitigación de riesgos por parte de los proveedores. Se espera que esto dé lugar a cambios en los servicios de plataformas incluso antes de que sea necesaria la incoación de un procedimiento de ejecución formal.

Habida cuenta de los recursos necesarios para emprender acciones legales contra las empresas sujetas al control del cumplimiento por parte de la Comisión, cualquier marco de control del cumplimiento debe garantizar que también se dedique tiempo a asegurar que se cumplan los requisitos procesales y se adopten todas las precauciones posibles, de modo que los casos se sostengan ante los tribunales en todas las instancias judiciales.

El enfoque basado en el riesgo y tecnológicamente neutro del Reglamento de Servicios Digitales es la base para unas medidas de ejecución preparadas para el futuro. Esto evoluciona gracias a los ciclos de evaluación de riesgos y auditoría de las plataformas, los compromisos conexos u otras respuestas a las medidas de ejecución, así como a la designación de nuevos servicios. La reciente apertura de una investigación contra X en relación con su sistema de IA, Grok, y el intercambio no consentido de imágenes íntimas (incluidas las generadas por la IA) demuestra cómo la aplicación del Reglamento de Servicios Digitales puede abarcar rápidamente nuevas prácticas o funciones problemáticas incorporadas a las plataformas en línea.

Del mismo modo, la reciente designación de WhatsApp como plataforma en línea de muy gran tamaño muestra cómo los servicios pueden entrar en el ámbito de aplicación del Reglamento de Servicios Digitales, al asumir las funciones y características de las plataformas en línea.

DECISIONES Y PROCEDIMIENTOS EN VIRTUD

DEL REGLAMENTO DE SERVICIOS DIGITALES

En el período transcurrido desde el comienzo de la aplicación del Reglamento de Servicios Digitales, la Comisión Europea y las autoridades nacionales han iniciado o completado una serie de medidas de ejecución relativas a la protección de los menores. Las decisiones y los procedimientos que se exponen a continuación sentaron las bases operativas con las que ahora se evalúa el cumplimiento de las plataformas. Esto seguirá evolucionando a medida que avancen las medidas de ejecución, por ejemplo para abarcar otros servicios y cuestiones, y se basará en una evaluación y mitigación continuas de los riesgos, así como en ciclos de auditoría.

En febrero de 2026, la Comisión Europea adoptó conclusiones preliminares según las cuales el diseño potencialmente adictivo de TikTok no cumple las normas de protección del Reglamento de Servicios Digitales. Estas conclusiones consideran que TikTok debe modificar el diseño básico de su servicio, por ejemplo, desactivando funciones clave que fomentan la adicción, como el «desplazamiento infinito por la pantalla», implantando «pausas en el tiempo de pantalla» efectivas (incluso durante la noche) y adaptando su sistema de recomendaciones²⁶³.

En marzo de 2026, la Comisión adoptó conclusiones preliminares contra cuatro plataformas pornográficas de muy gran tamaño (Pornhub, XNXX, Stripchat y XVideos) por no haber establecido una verificación adecuada de la edad²⁶⁴. Esto se complementó con una acción coordinada de la Junta Europea de Servicios Digitales contra plataformas de contenidos pornográficos más pequeñas²⁶⁵.

En abril de 2026, la Comisión Europea también publicó un informe preliminar en el que concluía que Meta había infringido la normativa por no impedir que menores de 13 años utilizaran Instagram y Facebook²⁶⁶.

Asimismo, se están llevando a cabo medidas coercitivas contra Snapchat para investigar la presunta inadecuación de los controles de verificación de edad y la configuración predeterminada, la insuficiencia de la protección de los menores frente a la captación sexual o para actividades delictivas y la ineficacia

de las herramientas de moderación de contenidos para impedir la difusión de información que dirija a los usuarios hacia la venta de productos ilegales, incluidas las drogas, y productos sujetos a restricciones de edad²⁶⁷.

Entre los compromisos aceptados, AliExpress ha acordado implantar un sistema por defecto que limite la visibilidad de los productos destinados a adultos, incluido el difuminado automático de las imágenes de dichos productos mediante un escaneo en tiempo real basado en IA²⁶⁸.

A escala nacional, la Autoridad de Consumidores y Mercados de los Países Bajos está investigando la plataforma de videojuegos Roblox en relación con los posibles riesgos a los que se enfrentan los menores en la plataforma²⁶⁹.

Se han incoado otros procedimientos sobre diseño adictivo, sistemas de recomendación, difusión de contenidos ilícitos (incluido el material de abuso sexual de menores) y medidas de protección en los mercados contra Facebook, Instagram, X en relación con Grok²⁷⁰, Shein²⁷¹ y Temu²⁷². Una investigación anterior sobre TikTok Lite dio lugar a la decisión de compromiso de la Comisión y a la retirada permanente de esta función del mercado de la UE.

Los efectos de las próximas medidas de ejecución relativas a los servicios y cuestiones mencionados anteriormente aclararán las expectativas concretas de la Comisión y establecerán un alto nivel de exigencia en materia de cumplimiento. Esto servirá de base para los cambios en la prestación de servicios, no solo de las plataformas en línea individuales objeto de investigación, sino también de todos los demás proveedores incluidos en el ámbito de aplicación del Reglamento de Servicios Digitales.

Para aprovechar todo el potencial del Reglamento de Servicios Digitales, ahora que esta arquitectura de aplicación está en funcionamiento, puede que sea necesario reforzarla aún más para garantizar que los casos de aplicación se tramiten con la rapidez y urgencia necesarias y que el Reglamento de Servicios Digitales surta pleno efecto. Para ello, todas las autoridades que participan en la aplicación a escala nacional y de la UE deben disponer de forma sistemática de los recursos adecuados para cumplir su mandato.

ESTRUCTURA DE APLICACIÓN DEL REGLAMENTO

DE INTELIGENCIA ARTIFICIAL

La estructura de aplicación del Reglamento de IA implica una competencia directa y centralizada de la Comisión en materia de aplicación en lo que respecta a los modelos de IA de uso general (incluidos los modelos de IA de uso general con riesgo sistémico) y los sistemas de IA basados en modelos de IA de uso general, cuando el modelo y el sistema hayan sido desarrollados por el mismo proveedor o por un proveedor que forme parte de la misma empresa.

El Reglamento omnibus digital sobre IA introduce una innovación adicional, ya que la aplicación relacionada con los sistemas de IA designados o integrados en plataformas en línea de muy gran tamaño o en motores de búsqueda en línea de muy gran tamaño en virtud del Reglamento de Servicios Digitales también se centraliza en la Comisión Europea. La aplicación de la normativa relativa a otros sistemas de IA incluidos en el ámbito de aplicación del Reglamento de IA es responsabilidad de las autoridades nacionales de vigilancia del mercado.

Las facultades de ejecución de la Oficina de IA de la UE y de las autoridades nacionales de vigilancia del mercado serán aplicables a partir del 2 de agosto de 2026. A partir de esta fecha, la Oficina de IA velará por el cumplimiento de las normas relativas a los modelos de IA de uso general²⁷³, los sistemas de IA de

uso general con riesgo sistémico²⁷⁴ y los sistemas de IA basados en modelos de IA de uso general cuando el modelo y el sistema hayan sido desarrollados por el mismo proveedor o por un proveedor que forme parte de la misma empresa, así como a los sistemas de IA integrados en plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño. Las obligaciones para los sistemas de IA de alto riesgo, tal como se acordó en el Ómnibus Digital sobre IA, empezarán a aplicarse en diciembre de 2027 (en el caso de los sistemas de IA independientes, como determinados sistemas de IA en el ámbito educativo) y en agosto de 2028 (en el caso de los sistemas de IA integrados en productos regulados, como los juguetes).

ESTRUCTURA DE APLICACIÓN DEL RGPD

El RGPD lo aplican las autoridades de protección de datos de cada Estado miembro de la UE, que están facultadas para investigar reclamaciones, llevar a cabo auditorías, ordenar medidas correctoras e imponer multas administrativas por infracciones de la legislación en materia de protección de datos.

Cuando una empresa (responsable del tratamiento de datos) trata datos personales en más de un Estado miembro, la autoridad de protección de datos principal, que es la autoridad de protección de datos del Estado miembro en el que la empresa tiene su establecimiento principal, es la responsable de la supervisión de dicha empresa.

La autoridad de control principal coopera y coordina sus acciones con las autoridades de control de la protección de datos de los demás Estados miembros de la UE en los que el tratamiento de datos tiene repercusiones. Esto se denomina «mecanismo de ventanilla única».

Las autoridades de protección de datos pueden iniciar investigaciones sobre la base de reclamaciones individuales, notificaciones obligatorias de violaciones de la seguridad de los datos, informes de los medios de comunicación o sus propias investigaciones. Las organizaciones que infrinjan las normas de protección de datos pueden enfrentarse a prohibiciones de tratamiento, órdenes de cumplimiento o multas de hasta 20 millones EUR o el 4 % del volumen de negocios anual mundial, si esta cifra es superior.

Tal como se establece en la Carta de los Derechos Fundamentales de la UE y se reitera en el RGPD, todas las autoridades de protección de datos deben ser independientes. Todos los Estados miembros deben garantizar que las autoridades de protección de datos dispongan de los recursos humanos, técnicos y financieros necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes.

El Comité Europeo de Protección de Datos (CEPD) reúne a todas las autoridades de control para garantizar la aplicación coherente del RGPD. Elabora orientaciones sobre la aplicación del RGPD. El CEPD está elaborando actualmente directrices sobre el tratamiento de los datos de los niños. El CEPD también promueve la cooperación entre las autoridades de protección de datos.

El RGPD es tecnológicamente neutro y adopta un enfoque basado en el riesgo. Esto significa que las organizaciones deben aplicar las medidas técnicas y organizativas pertinentes, proporcionales al riesgo que plantean sus actividades de tratamiento de datos.

A finales del año pasado, se aprobó el Reglamento de procedimiento del RGPD. Este introdujo nuevas normas para mejorar la cooperación entre los organismos nacionales de protección de datos a la hora de hacer cumplir el RGPD, a fin de agilizar el proceso de tramitación de las reclamaciones transfronterizas en materia de protección de datos. En mayo de 2025, las autoridades de protección de datos publicaron la

Declaración de Helsinki sobre una mayor claridad, apoyo y compromiso. En esta declaración, acordaron mejorar la coherencia en la aplicación y el cumplimiento del RGPD.

MEDIDAS Y PROCEDIMIENTOS DE EJECUCIÓN

DEL RGPD SELECCIONADOS

El RGPD está en vigor desde 2018. Desde entonces, se han impuesto multas por valor de más de 7 000 millones EUR a organizaciones por infringir las normas de protección de datos²⁷⁵. Las autoridades de protección de datos pueden hacer uso de sus competencias para exigir a las empresas que adapten sus actividades de tratamiento a la normativa. Esto permite a las autoridades de protección de datos colaborar con los responsables del tratamiento antes de iniciar una investigación, lo que ahorra tiempo y recursos.

Por ejemplo, en febrero de 2023, la Comisión de Protección de Datos de Irlanda colaboró con Meta en relación con el etiquetado en Instagram. Cuando un niño quería etiquetar una cuenta pública a la que no seguía, recibía el mensaje «No se ha podido etiquetar la cuenta. Haz pública tu cuenta para etiquetar a otras que no te sigan»²⁷⁶.

Esta notificación también incluía un botón «Ir a ajustes» que llevaba al usuario a un menú en el que podía cambiar su cuenta de privada a pública. Esta configuración no advertía a los niños de las posibles consecuencias de este cambio, ni les redirigía a ninguna pregunta frecuente o artículo del centro de ayuda.

Tras las conversaciones con el responsable del tratamiento de datos, se introdujeron cambios en las notificaciones a los usuarios. La notificación se actualizó para que incluya el siguiente mensaje: «No se ha podido etiquetar la cuenta. Tu cuenta es privada, por lo que solo puedes etiquetar a tus seguidores. Puedes gestionar tu privacidad en Ajustes».

«Ir a ajustes» se sustituyó por un botón «Más información» que lleva a los usuarios a un artículo del centro de ayuda en el que pueden averiguar cómo convertir su cuenta de usuario en privada en cualquier momento, las diferencias entre las cuentas privadas y públicas, cómo pueden los usuarios gestionar la privacidad en Instagram e información para los progenitores sobre «quién puede ver las publicaciones de mi hijo adolescente en Instagram».

Las autoridades de protección de datos han adoptado múltiples decisiones sobre infracciones del RGPD relacionadas con los datos de menores. También han promulgado prohibiciones de tratamiento que impiden a un responsable del tratamiento tratar los datos personales de los interesados, incluidos los de los niños, hasta que dicho tratamiento se ajuste a los requisitos del RGPD. A continuación se destaca una selección de estas medidas.

Varias autoridades de protección de datos han iniciado investigaciones contra los responsables del tratamiento por incumplir el principio de protección de datos desde el diseño y por defecto. Por ejemplo, la Comisión de Protección de Datos de Irlanda impuso a TikTok una multa de 345 millones EUR, ya que se constató que infringía varias disposiciones del RGPD.

Entre ellas se incluían la protección de datos desde el diseño y por defecto, así como el principio de minimización de datos. La Comisión de Protección de Datos determinó que TikTok infringía estas disposiciones, ya que, por defecto, hacía que las cuentas de los menores fueran públicas para cualquier persona, tanto dentro como fuera de TikTok.

La Comisión de Protección de Datos de Irlanda también constató que TikTok utilizaba patrones oscuros para incitar a los niños a optar por cuentas públicas por defecto. Esto significaba que cualquier persona podía ver su contenido, lo que infringía la protección de datos desde el diseño y por defecto, así como el principio de equidad. Asimismo, constató que TikTok no se aseguraba de que los usuarios adultos que supervisaban la cuenta de un menor a través de la «vinculación familiar» estuvieran verificados como progenitores o tutores del niño²⁷⁷.

Además, la Comisión de Protección de Datos de Irlanda impuso a Instagram una multa de 450 millones EUR, ya que constató que había infringido el principio de protección de datos desde el diseño y por defecto. Instagram había permitido a los menores crear cuentas de empresa, que estaban obligadas a mostrar datos de contacto accesibles al público en su perfil. La Comisión de Protección de Datos determinó que Instagram vulneraba este principio, ya que todas las cuentas de usuario estaban configuradas como públicas por defecto. Esto significaba que cualquier persona podía ver el contenido del menor, a menos que modificara la configuración²⁷⁸.

La autoridad italiana de protección de datos impuso una prohibición temporal de las actividades de tratamiento de TikTok debido a preocupaciones sobre la seguridad de los menores, en particular tras la muerte de una niña italiana de 10 años. La prohibición impuso una limitación inmediata a las actividades de tratamiento de TikTok en el caso de los usuarios cuya edad no pudiera determinarse con certeza. Esto llevó a la plataforma a volver a verificar la edad de sus usuarios italianos y a cerrar más de medio millón de cuentas sospechosas de pertenecer a menores de 13 años, la edad a partir de la cual TikTok permite que los niños utilicen su servicio²⁷⁹.

A principios de este año, la Comisión de Protección de Datos de Irlanda inició una investigación sobre X en relación con la creación de imágenes sexualizadas sin consentimiento, también de menores, mediante la herramienta de IA Grok. La Comisión de Protección de Datos examinará el cumplimiento por parte de X de varios artículos, entre ellos la minimización de datos y la protección de datos desde el diseño y por defecto²⁸⁰.

APLICACIÓN DE LA DIRECTIVA DE SERVICIOS DE COMUNICACIÓN

AUDIOVISUAL Y PROTECCIÓN DE LOS MENORES EN LÍNEA

La protección de los menores es un ámbito prioritario para la aplicación por parte de los reguladores de los medios de comunicación. En 2024, el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual (ERGA) evaluó las medidas adoptadas por los reguladores de los medios de comunicación en relación con la protección de los menores. Llegó a la conclusión de que era necesario establecer y perfeccionar los criterios para clasificar los contenidos nocivos para los menores.

Un ejemplo de la aplicación de la Directiva de Servicios de Comunicación Audiovisual en relación con las plataformas de intercambio de vídeos en lo que respecta a la protección de los menores puede encontrarse en Italia. La AGCOM, la Autoridad Reguladora de la Comunicación de Italia, detectó la presencia en TikTok de vídeos sobre la «cicatriz francesa». De conformidad con la normativa sobre las plataformas de intercambio de vídeos, la AGCOM inició un procedimiento de intervención que llevó a TikTok, una plataforma de intercambio de vídeos con sede en Irlanda, a retirar los vídeos.

El regulador alemán DLM ha adoptado medidas contra plataformas pornográficas establecidas en Chipre y Chequia. El procedimiento transfronterizo se basó en la Directiva sobre el comercio electrónico, tal como se prevé en la Directiva de Servicios de Comunicación Audiovisual. La base jurídica era el Tratado

interestatal sobre la protección de menores en los medios de comunicación (JMStV), que transpone la Directiva de Servicios de Comunicación Audiovisual, y la disposición pertinente era la prohibición de distribuir pornografía a menores y las normas sobre la verificación de la edad.

El Reglamento Europeo sobre la Libertad de los Medios de Comunicación²⁸¹, que establece un procedimiento transfronterizo para solicitar el cumplimiento de las obligaciones de las plataformas de intercambio de vídeos establecidas en otro Estado miembro, también se ha activado en relación con varias plataformas pornográficas establecidas en Chipre. Esto ha llevado a las plataformas en cuestión a respetar las obligaciones de la Directiva de Servicios de Comunicación Audiovisual en materia de protección de los menores, incluida la verificación de la edad. El regulador chipriota está evaluando actualmente las respuestas facilitadas por los proveedores pertinentes (Stripchat) sobre cómo han implantado la verificación de la edad en varios países, por ejemplo, Alemania.

RED DEL REGLAMENTO SOBRE LA COOPERACIÓN EN MATERIA DE PROTECCIÓN DE LOS CONSUMIDORES (CPC)

Tal como se establece en la Agenda del Consumidor 2030, la Comisión Europea propondrá una revisión del Reglamento sobre la cooperación en materia de protección de los consumidores (CPC) para reforzar aún más la aplicación de la legislación en materia de protección de los consumidores. Esto podría contribuir a centralizar las facultades de ejecución directas en casos específicos a escala de la UE.

De este modo, la aplicación del Reglamento CPC sería más rápida y tendría un mayor efecto disuasorio. Además, contribuiría a proteger mejor a los menores que, debido a su mayor vulnerabilidad y falta de experiencia, corren un alto riesgo de verse expuestos a prácticas comerciales desleales en línea.

MEDIDAS DE EJECUCIÓN SELECCIONADAS DE LA RED CPC

En lo que respecta al sector digital, en marzo de 2025 la Comisión Europea publicó la posición común de la Red CPC sobre Star Stable Online²⁸². La Red constató infracciones de la DPCD y la DDC, como la incitación a los niños a comprar o convencer a los adultos de que les compren moneda o artículos dentro de videojuegos; patrones oscuros (alegaciones de escasez con respecto a monedas virtuales o contenidos dentro del juego); la falta de información clara y transparente, adaptada a los niños, sobre la compra y el uso de monedas virtuales dentro del juego, y la falta de divulgación del carácter comercial de contenidos publicados por influencers. Actualmente, la Comisión está facilitando el diálogo entre la Red CPC y la empresa para poner fin a estas infracciones de la legislación de la UE en materia de protección de los consumidores.

En marzo de 2025, la Comisión publicó los principios clave de la Red CPC sobre las monedas virtuales dentro del juego, que reflejan la interpretación común de las autoridades CPC de la legislación vigente de la UE en materia de protección de los consumidores (principalmente la DPCD y la DDC). Estos principios clave tienen por objeto promover la transparencia y la equidad en el uso por parte de la industria de los videojuegos de monedas virtuales que se pueden adquirir, y garantizar que se respeten las vulnerabilidades de los consumidores, especialmente las de los niños²⁸³.

El tema de la comercialización por parte de influencers es de gran interés para la Red CPC, especialmente cuando estas prácticas afectan a los niños. En 2023, las autoridades CPC nacionales de 22 Estados miembros llevaron a cabo una inspección de las publicaciones de 576 influencers para verificar si revelaban sus actividades publicitarias, tal como exige la legislación de la UE en materia de protección

de los consumidores. Como resultado de la inspección, el 62 % de los influyentes controlados fueron seleccionados para una investigación más exhaustiva²⁸⁴. La Comisión Europea también ha puesto en marcha el Influencer Legal Hub (Centro Legal para Influyentes), donde los influyentes pueden encontrar información práctica sobre el cumplimiento del Derecho de la UE²⁸⁵.

En febrero de 2022, se puso en marcha una acción coordinada de la Red CPC contra TikTok. Abordó las preocupaciones de las autoridades CPC relacionadas con la publicidad encubierta, las técnicas publicitarias agresivas dirigidas a los niños y determinadas cláusulas contractuales de las políticas de TikTok que podrían considerarse engañosas y confusas para los consumidores.

En junio de 2022, TikTok se comprometió a adaptar sus prácticas a las normas de la UE en materia de publicidad y protección de los consumidores²⁸⁶. Las autoridades CPC están supervisando el cumplimiento de TikTok, en particular si sus prácticas comerciales (por ejemplo, la publicidad) son suficientemente transparentes para que los niños comprendan su naturaleza.

EDUCACIÓN DE LOS CONSUMIDORES Y VÍAS DE RECURSO

Gracias a la reciente adopción de la Directiva 2025/2647/UE, que revisa la Directiva sobre resolución alternativa de litigios, los consumidores pueden recurrir a la resolución extrajudicial de litigios para resolver los litigios relacionados con los servicios y contenidos digitales, así como aquellos relacionados con la información precontractual cuando se haya formalizado un contrato.

La ampliación del ámbito de aplicación de la Directiva adaptó la resolución extrajudicial de litigios a la era digital al garantizar que se pudieran resolver de esta manera más litigios en materia de consumo. Un ejemplo podría ser un litigio relacionado con una suscripción a un videojuego o con la descripción facilitada sobre un producto dirigido a menores. La Directiva relativa a las acciones de representación permite a las entidades cualificadas designadas, como las organizaciones de consumidores y los organismos públicos, interponer acciones legales para la protección de los intereses colectivos de los consumidores. Esto incluye a los menores afectados por prácticas ilícitas de los comerciantes.

Las acciones pueden tener por objeto el cese de las prácticas ilícitas y el recurso colectivo de los consumidores. Pueden interponerse acciones para hacer valer los derechos de los consumidores contemplados en más de setenta actos de la UE enumerados en el anexo I de la Directiva, como la Directiva sobre las prácticas comerciales desleales, el RGPD, el Reglamento de Mercados Digitales, el Reglamento de Servicios Digitales o el Reglamento de IA. Siempre que los legisladores de la UE examinen un nuevo instrumento de la UE pertinente para la protección de los intereses colectivos de los consumidores, podrá añadirse al anexo, lo que permitirá su aplicación a través del modelo de la UE de recurso colectivo de los consumidores.

Asuntos pendientes

NO SE ABORDA SUFICIENTEMENTE EL DISEÑO NOCIVO

Si bien la aplicación de la legislación vigente se encuentra en muchos casos en sus fases iniciales, se espera que, con el tiempo y recursos suficientes, suponga un cambio en el modelo de negocio de los proveedores de medios sociales y otros servicios digitales, al definir qué elementos de este modelo son, en última instancia, compatibles con los derechos fundamentales en la UE, incluidos los derechos del niño.

Un claro ejemplo de ello es la prohibición de la publicidad basada en la elaboración de perfiles de menores. Al igual que la prohibición de la publicidad basada en la elaboración de perfiles utilizando categorías especiales de datos sensibles, esta prohibición rechaza directamente la aceptabilidad de una práctica que constituye el núcleo del modelo de negocio de varias plataformas.

Otro ejemplo son las obligaciones de evaluación y mitigación de riesgos impuestas a los proveedores de medios sociales y otros servicios digitales. Estas obligaciones exigen a los proveedores seguir invirtiendo para comprender los riesgos que sus servicios plantean para los derechos fundamentales, incluidos los derechos del niño, y prevenir y mitigar estos riesgos.

A pesar de ello, persisten varias deficiencias. En primer lugar, la legislación vigente de la UE suele basarse en prácticas enumeradas (por ejemplo, características adictivas específicas). Esto genera un desfase estructural. Un enfoque basado en características puede dar lugar a lagunas normativas, ya que los servicios digitales evolucionan con el tiempo más allá de las características específicamente enumeradas y abordadas en la legislación. Esta evolución puede producirse de forma intencionada para evitar la aplicación por parte de los reguladores.

Además, los riesgos suelen ser transversales y no surgen de una única característica o funcionalidad aislada, sino de la interacción de múltiples características o del diseño de un servicio en general. Piénsese en las nuevas formas de contenido audiovisual. Los entornos inmersivos basados en la tecnología de realidad extendida y los vídeos de corto formato con reproducción automática, por ejemplo, han creado riesgos para los niños que no se previeron cuando se adoptaron los instrumentos legislativos pertinentes.

La legislación puede adaptarse durante la aplicación, como demuestran la investigación sobre X/Grok en el marco del Reglamento de Servicios Digitales y la designación de WhatsApp como plataforma en línea de muy gran tamaño. Sin embargo, esta adaptación se produce característica por característica, después de que se haya detectado el daño, al ritmo de los procedimientos formales de ejecución.

Además, la legislación vigente de la UE aborda la actividad principal de las plataformas de manera indirecta, al proporcionar un marco basado en los derechos fundamentales dentro del cual debe operar cualquier modelo de negocio. A modo de ejemplo, los proveedores de plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño deben cumplir requisitos específicos de transparencia y diseño relacionados con los sistemas de recomendación²⁸⁷, y los proveedores de plataformas en línea de muy gran tamaño están obligados a ofrecer al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles²⁸⁸; sin embargo, la forma concreta en que deben o no deben diseñar sus sistemas de recomendación puede determinarse en el marco de una medida de ejecución.

En la actualidad, los reguladores suelen encontrarse «a la defensiva» al intentar hacer cumplir la legislación en un entorno de medios sociales+ en rápida evolución, en el que pueden definirse carac-

«Nuestro objetivo no es excluir a los niños, sino garantizar que el mundo digital se adapte a ellos a medida que crecen. Si los proveedores de tecnología quieren acceder a nuestros niños, tendrán que demostrar que cumplen los requisitos.»

— LEANDA BARRINGTON-LEACH,
DIRECTORA EJECUTIVA, FUNDACIÓN
5 RIGHTS

terísticas y funcionalidades explícitas que siguen evolucionando, después de que los servicios digitales se hayan introducido en el mercado. Esto puede exponer a millones de usuarios, incluidos niños y adolescentes, a riesgos de sufrir daños. En algunos casos, los riesgos solo pueden materializarse o quedar claros después de la introducción de los servicios en el mercado, por ejemplo, debido a cómo se utilizan estas características o funcionalidades en la práctica o en función del contexto. En términos de ejecución, a la hora de impugnar ante los proveedores el incumplimiento de sus obligaciones de diligencia debida, la carga de la prueba puede recaer actualmente, con frecuencia, sobre los organismos de ejecución de la UE y nacionales, que deben demostrar que los medios sociales y otros servicios digitales son perjudiciales mediante procesos judiciales prolongados y costosos contra grandes empresas muy equipadas.

Por lo tanto, podría convertirse en norma que los proveedores de medios sociales y otros servicios digitales que lancen, gestionen o actualicen servicios que puedan plantear riesgos para los niños y adolescentes deban demostrar, antes de la implantación en el mercado, que sus servicios o nuevas funcionalidades son seguros para que los menores los utilicen.

ENFOQUES NACIONALES DIVERGENTES SOBRE LAS RESTRICCIONES

DE EDAD Y EL CONSENTIMIENTO DE LOS NIÑOS

La cuestión de la edad es la laguna normativa más evidente en la legislación vigente. Deben tenerse en cuenta dos aspectos. En primer lugar, el RGPD ha fijado, de manera general, los 16 años como edad mínima para que los menores puedan dar su consentimiento a los «servicios de la sociedad de la información» para el tratamiento de sus datos personales. El RGPD ofrece a los Estados miembros la posibilidad de reducir esta edad a cualquier edad comprendida entre los 13 y los 16 años. Si el niño es menor de 16 años (o de otra edad establecida por un Estado miembro), el tratamiento solo será lícito si el consentimiento lo da o autoriza el titular de la responsabilidad parental.

En segundo lugar, varios Estados miembros de la UE están legislando, o estudiando la posibilidad de legislar, sobre las restricciones de edad para que los menores accedan a los medios sociales y otros servicios digitales, y algunos incluso adoptan enfoques distintos con respecto a los umbrales de consentimiento de la UE y de los Estados miembros. Los enfoques de los Estados miembros con respecto a las edades mínimas difieren en cuanto al alcance, el umbral de edad y los servicios incluidos, así como la posibilidad de que el consentimiento parental pueda prevalecer sobre dicho umbral.

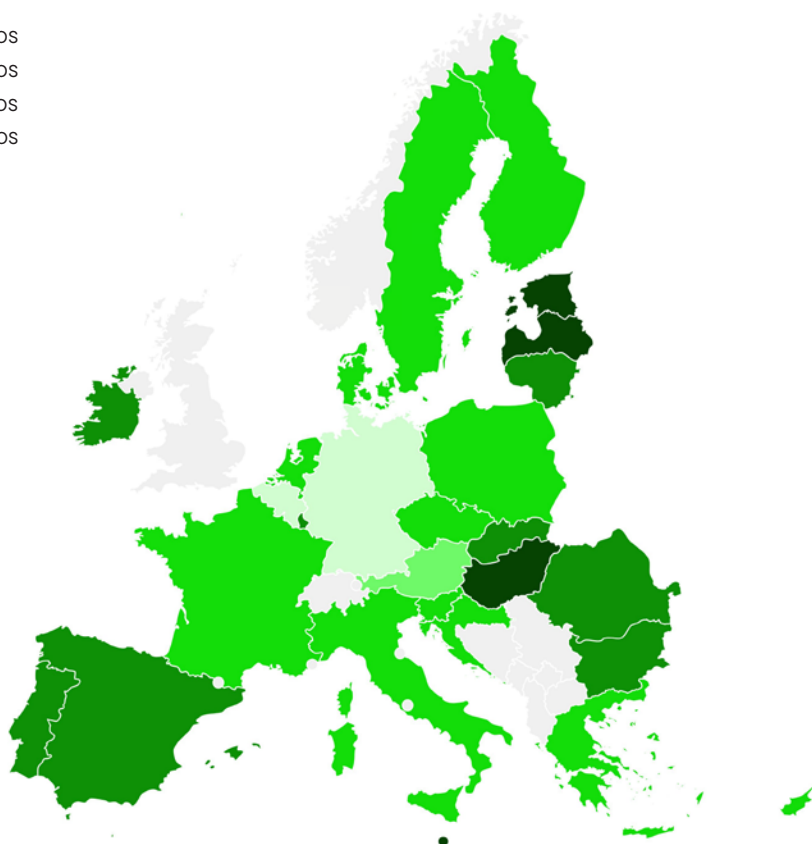
La proliferación de iniciativas nacionales que establecen restricciones de edad para acceder a los medios sociales y otros servicios digitales plantea riesgos relacionados con la fragmentación del mercado único y los niveles desiguales de protección de los menores en toda la UE. Varios Estados miembros, entre ellos Austria, Chipre, Dinamarca, Francia, Luxemburgo, Grecia, España y Eslovenia, piden un enfoque a escala de la UE de las restricciones de edad para acceder a los medios sociales+.

La Declaración de Jutlandia, firmada en octubre de 2025 por veinticinco Estados miembros a iniciativa de la Presidencia danesa del Consejo, pedía un entorno digital más seguro para los menores, en particular mediante la verificación de la edad y evaluaciones de la edad a la que debe permitirse a los menores acceder a los medios sociales y otros servicios digitales. Las Conclusiones del Consejo Europeo de 23 de octubre de 2025 y las Conclusiones del Consejo Europeo de 19 de marzo de 2026 destacan la importancia de proteger a los menores en línea.

Se están celebrando debates en todos los Estados miembros, ya sea en los parlamentos nacionales, los gobiernos o la sociedad civil, centrados en la introducción de restricciones de edad a distintos niveles. Las restricciones propuestas oscilan entre los 13 y los 16 años, permitiendo a veces diferentes niveles de edad, con o sin consentimiento parental. Italia, Francia y Grecia han notificado oficialmente a la Comisión sus proyectos de ley a través del Sistema de Información sobre Reglamentos Técnicos (TRIS).

Gráfico 1: Estados miembros de la UE que proponen o están estudiando la posibilidad de establecer restricciones de edad para los medios sociales y otros servicios digitales

- Mayores de 16 años
- Mayores de 15 años
- Mayores de 14 años
- Mayores de 13 años
- No procede



Francia, Italia y Dinamarca están considerando restricciones para menores de 15 años. Chipre y Rumanía proponen un límite de 16 años, y Alemania, de 13. Grecia y Dinamarca proponen dos niveles: acceso restringido para menores de 15 años y acceso solo con el consentimiento de los progenitores para los jóvenes de entre 12 y 15 años (de 13 a 15 en el caso de Dinamarca).

Dado que muchos Estados miembros están estudiando la posibilidad de establecer una edad mínima para los medios sociales+, con ámbitos de aplicación divergentes, y obligaciones complementarias, sería importante adoptar un enfoque armonizado a escala de la UE para garantizar que los menores se beneficien del mismo nivel de protección en línea en toda la UE. Para garantizar un mismo nivel de protección, también es fundamental examinar cómo pueden relacionarse las posibles restricciones de edad con las medidas de seguridad, en particular las impuestas por la legislación de la UE, incluido el Reglamento de Servicios Digitales.

«Una edad mínima clara a escala de la UE serviría, a corto plazo, de apoyo a los progenitores, reduciría la presión social y de los compañeros sobre los niños y crearía un fuerte incentivo para que las plataformas rediseñen sus servicios en consonancia con la seguridad y el bienestar de los niños.»

— LIES CRAEYNST, FUNDADORA,
KIDSUNPLUGGED

Las restricciones de edad propuestas por los Estados miembros pueden estar relacionadas con los riesgos específicos que presentan los distintos tipos de medios sociales y otros servicios digitales, o tratar de abordarlos. Para garantizar un mismo nivel de protección de los menores, un enfoque armonizado de la verificación de la edad debe ir acompañado de medidas de seguridad aplicadas eficazmente por los reguladores y de funciones de seguridad implantadas por los proveedores de medios sociales y otros servicios digitales (ya sea mediante un enfoque de seguridad desde el diseño o por defecto).

ENFOQUES SOBRE LAS RESTRICCIONES DE EDAD Y EL CONSENTIMIENTO

Estado miembro	Situación de los debates nacionales y posibles medidas sobre las restricciones de edad para los servicios digitales	Edad mínima propuesta o considerada	Edad de los niños para el consentimiento en relación con el tratamiento de datos en línea
Bélgica	En abril de 2026, el Gobierno flamenco aprobó un anteproyecto de decreto por el que se introduce un límite de edad legal de 13 años para determinadas plataformas en línea que pueden ser perjudiciales para los menores.	13	13
Bulgaria	En mayo de 2026, un partido político que no está representado en el Gobierno propuso enmiendas a la Ley de Protección de la Infancia para restringir el acceso de los menores de 16 años a los medios sociales. El acceso podría permitirse a partir de los 13 años con el consentimiento de los padres.	16	14
Chequia	Todavía no hay ninguna propuesta. El partido gobernante ANO (PřE) tiene previsto proponer este año una nueva legislación para prohibir a los niños menores de 15 años.	15	15
Dinamarca	Propuesta legislativa en fase de elaboración. En noviembre de 2025, el Gobierno anunció un acuerdo político sobre la prohibición para los niños menores de 15 años para acceder a los medios sociales, aunque el acceso podría permitirse a partir de los 13 años con el consentimiento de los padres.	15	15
Estonia	Oposición general a la idea de imponer restricciones de edad en los medios sociales.	No procede	13
Alemania	Hasta la fecha no se ha presentado ninguna propuesta legislativa. En noviembre de 2025, el Gobierno declaró que, en principio, apoyaba una posible regulación y creó un comité de expertos, que publicó su informe el 24 de junio, en el que proponía un límite mínimo de 13 años y limitaciones al acceso al mercado para los servicios que no son seguros, y pedía un enfoque a escala de la UE. Los partidos políticos y las ONG han presentado varias propuestas.	13	16
Irlanda	Todavía no hay ninguna iniciativa legislativa. Tánaiste (viceprimer ministro) ha expresado su apoyo a la restricción del acceso a los medios sociales para los menores de 16 años. El Comité Mixto de Arte, Medios de Comunicación, Comunicaciones, Cultura y Deporte no apoyó dicha prohibición en mayo de 2026.	16	16
Grecia	Se espera que la ley se vote en el verano de 2026 y se aplique a partir de enero de 2027.	15	15
España	En abril de 2025, el Gobierno de España presentó una propuesta legislativa para aumentar la edad de consentimiento de los niños para el tratamiento de sus datos personales. En febrero de 2026, el presidente anunció que España prohibirá el acceso a las plataformas digitales a los menores de 16 años.	16	14
Francia	Propuesta legislativa presentada en 2025 (ambas cámaras parlamentarias han adoptado sus posiciones, pero aún tienen que llegar a un acuerdo sobre el texto transaccional). Entrada en vigor prevista de la ley en septiembre de 2026. Francia propone un régimen diferenciado, con una prohibición para los menores de 15 años de determinados servicios de medios sociales designados como perjudiciales y el consentimiento parental para el acceso a otros servicios de medios sociales.	15	15

Estado miembro	Situación de los debates nacionales y posibles medidas sobre las restricciones de edad para los servicios digitales	Edad mínima propuesta o considerada	Edad de los niños para el consentimiento en relación con el tratamiento de datos en línea
Croacia	Propuesta legislativa presentada en 2025 pero rechazada en marzo de 2026.	15	16
Italia	El Gobierno está preparando una iniciativa legislativa para prohibir a los menores de 15 años el acceso a los medios sociales. Paralelamente, en 2024 y 2026 se presentaron dos iniciativas parlamentarias distintas, pero actualmente no avanzan, ya que el presidente del Consejo declaró que la prohibición podría no ser la opción preferida.	15	14
Chipre	Iniciativa legislativa anunciada por el Gobierno en 2026.	15	14
Letonia	Todavía no hay ninguna propuesta legislativa. En marzo de 2026, la coalición gubernamental acordó elaborar una norma para restringir el acceso a los medios sociales por debajo de una determinada edad.	No procede	13
Lituania	Propuesta legislativa presentada en 2026.	16	14
Luxemburgo	Resolución del Parlamento Europeo (enero de 2026) en la que se pide la creación de un marco de la UE o la coordinación de acciones con BE, DE y FR.	16.	16.
Hungría	Todavía no hay ninguna propuesta.	No procede	16
Malta	En febrero de 2026 se celebró una consulta pública sobre la reforma de los medios sociales. Actualmente en fase posterior a la consulta.	No procede	13
Países Bajos	Los planes de coalición (enero de 2026) piden que se establezca a escala de la UE una edad mínima para acceder a los medios sociales.	15	16
Austria	Anuncio del Gobierno Federal; propuesta legislativa prevista para el verano de 2026.	14	14
Polonia	Anuncios de algunos diputados de la Cámara Baja del Parlamento (Sejm) y del Ministerio de Asuntos Digitales.	15.	16.
Portugal	Preparación de una iniciativa legislativa parlamentaria en 2026 (fase de audiencia).	16	13
Rumanía	En 2025 se publicó una propuesta legislativa sobre la edad en la que se alcanzaría la mayoría digital. Otras también se están debatiendo en diferentes fases del procedimiento.	15 - 16	16
Eslovenia	En febrero de 2026, el Gobierno anunció los preparativos para regular el uso de los medios sociales por parte de los niños hasta los 15 años.	15	15
Eslovaquia	Propuesta legislativa anunciada en 2026 por el Ministerio de Inversiones, Desarrollo Regional e Informática.	16	16
Finlandia	El primer ministro y su partido publicaron en noviembre de 2025 un documento estratégico en apoyo de la prohibición de que los menores de 15 años accedan a los medios sociales. Las recomendaciones nacionales apoyan que los menores de 13 años no utilicen los medios sociales.	15	13
Suecia	El Gobierno creó una Comisión para investigar la posibilidad de prohibir el acceso de los niños a las redes sociales por debajo de una determinada edad, y dicha Comisión propuso establecer un límite a los 15 años para el uso de los medios sociales.	15	13

ADOPCIÓN DE LA SOLUCIÓN DE LA UE PARA LA VERIFICACIÓN DE LA EDAD POR PARTE DE LOS ESTADOS MIEMBROS

La solución de la UE para la verificación de la edad es técnicamente muy avanzada y su plan director está listo para que los Estados miembros y los agentes del mercado lo adapten a sus necesidades. Sin embargo, la eficacia de estas herramientas para reforzar la protección infantil en línea vendrá determinada, en última instancia, por su adopción real por parte de los Estados miembros, los agentes del mercado y los proveedores de medios sociales y otros servicios digitales.

La designación de proveedores de prueba de la edad de confianza también es esencial para el funcionamiento eficaz de la solución de la UE para la verificación de la edad. A pesar de los reiterados llamamientos de la Comisión Europea, muchos Estados miembros aún no han actuado para designar proveedores de prueba de la edad de confianza.

No es posible aplicar una restricción de edad armonizada a escala de la UE para el acceso a los medios sociales y otros servicios digitales sin un ecosistema de verificación de la edad que pueda utilizarse para demostrar la edad de los menores. La actual solución de la UE para la verificación de la edad puede ampliarse técnicamente de los mayores de 18 años a otras edades, incluidos, por ejemplo, los adolescentes, en consonancia con la legislación nacional.

Sin embargo, sin proveedores de prueba de la edad de confianza que puedan expedir credenciales de edad a menores, los proveedores de medios sociales y otros proveedores de servicios digitales corren el riesgo de recurrir a otros métodos menos sólidos (por ejemplo, la autodeclaración) o menos respetuosos de la privacidad, y los Estados miembros pueden tener dificultades para garantizar una verificación eficaz de la edad.

NECESIDADES DE APLICACIÓN:

CAPACIDAD, RAPIDEZ Y COORDINACIÓN ENTRE REGULADORES

La aplicación hasta la fecha demuestra que los instrumentos legislativos existentes pueden dar lugar a decisiones y cambios visibles en el cumplimiento. También pone de relieve varios retos.

Una aplicación eficaz es fundamental para garantizar la seguridad infantil en línea. Esto requiere competencias suficientes y autoridades dotadas de recursos adecuados. En la práctica, las arquitecturas de aplicación contradictorias pueden generar varios problemas. Entre ellos se incluyen la dispersión de unos recursos ya de por sí limitados, el tiempo de puesta en marcha, una mayor complejidad y competencias potencialmente contrapuestas o solapadas. Estos problemas pueden desincentivar el cumplimiento o incluso ofrecer posibles motivos para que los proveedores de medios sociales y otros servicios digitales eludan o retrasen dicho cumplimiento.

Un reto importante para los reguladores es mantener una dotación de personal adecuada con los conocimientos especializados necesarios. A medida que las operaciones de los proveedores se vuelven cada vez más complejas, los reguladores deben asegurarse de contar con suficiente personal debidamente cualificado para evaluar de manera eficaz si los medios sociales y otros servicios digitales cumplen la legislación. Esto se aplica tanto a escala nacional como de la UE.

En términos más generales, la disponibilidad y coordinación de los recursos humanos y financieros asignados a los sistemas de protección de la infancia (también para apoyar la aplicación pública) constituyen

otro desafío²⁸⁹. Invertir la carga de la prueba en materia de aplicación, como se ha mencionado anteriormente, puede contribuir a mejorar la capacidad de aplicación y a obtener mejores resultados, sin ejercer una presión adicional sobre los limitados recursos de los reguladores, tanto a escala nacional como de la UE.

LAGUNA EN MATERIA DE SEGURIDAD INFANTIL:

ABUSO Y EXPLOTACIÓN SEXUALES EN LÍNEA

El Reglamento provisional, aplicable desde 2021 hasta el 3 de abril de 2026, estableció normas temporales que establecían excepciones a determinadas obligaciones de la Directiva sobre la privacidad y las comunicaciones electrónicas. Esto permitió a los proveedores de determinados servicios de comunicaciones interpersonales utilizar tecnologías para el tratamiento de datos personales y de otro tipo con el fin de detectar y denunciar el material de abuso sexual de menores y la captación sexual, así como eliminar dicho material de sus servicios.

En diciembre de 2025, la Comisión Europea propuso una prórroga del Reglamento provisional hasta 2028 como solución temporal a la espera de la adopción del Reglamento a largo plazo para prevenir y luchar contra el abuso sexual de menores. Sin embargo, el Parlamento Europeo y el Consejo no llegaron a un acuerdo sobre la propuesta. Como consecuencia de ello, el Reglamento provisional dejó de aplicarse el 3 de abril de 2026, lo que generó inseguridad jurídica a escala de la UE.

Debe encontrarse una solución lo antes posible en el Reglamento a largo plazo para la detección del abuso sexual de menores en las comunicaciones privadas, donde se produce la mayoría de estos delitos. La detección proactiva por parte de los prestadores de estos servicios ha sido la principal fuente de investigaciones sobre el abuso sexual de menores durante más de 15 años.

El alcance de la detección debe abarcar no solo el material conocido de abuso sexual de menores para evitar la revictimización, sino también el material nuevo, que a menudo indica abusos en curso, e incluir el material generado por IA. Este último ha aumentado exponencialmente en los últimos años (de 5 000 denuncias en 2023 a 1,3 millones en 2025). La detección también debe incluir la captación sexual para prevenir abusos inminentes y poner fin a los abusos en curso, que también han aumentado de forma exponencial (se han multiplicado por doce en los últimos tres años).

Otras lagunas de la legislación actual se refieren a las formas emergentes de abuso y explotación sexuales de menores vinculadas a los avances tecnológicos, como el material de abuso sexual de menores generado por IAⁱ, la captación sexual en línea, la retransmisión en directo de abusos, la difusión de instrucciones sobre cómo cometer infracciones y la gestión de un servicio en línea con fines de abuso sexual de menores. Estas cuestiones se abordan en la propuesta de revisión del marco del Derecho penal (Directiva 2011/93/UE).

i. A fin de garantizar una mayor protección de los derechos de los niños, el Parlamento Europeo y el Consejo han acordado, en el marco del Ómnibus Digital sobre IA, incluir una prohibición de los sistemas de IA que generen contenidos íntimos sin consentimiento y material de abuso sexual de menores. Esta prohibición se aplicará a partir del 2 de diciembre de 2026.

Recomendaciones

RECOMENDACIÓN N.º 1

Proponer una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años

Una restricción del acceso a los medios sociales y otros servicios digitales armonizada a escala de la UE para los menores de 13 años. Una restricción armonizada del acceso facilitaría la aplicación de mecanismos de control de la edad proporcionados y respetuosos de los derechos, e impulsaría los requisitos de seguridad desde el diseño para los proveedores de medios sociales y otros servicios digitales. Los menores de 13 años deben tener un acceso de duración limitada a entornos de medios sociales+ adecuados a su edad, únicamente con autorización y supervisión parental o en contextos educativos. A partir de los 13 años, el uso que hacen los adolescentes de los medios sociales y otros servicios digitales adecuados a su edad y seguros debe poder evolucionar hacia la autonomía.

Unas normas armonizadas a escala de la UE sobre una edad mínima de 13 años contribuirían al correcto funcionamiento del mercado único al garantizar un marco único de cumplimiento para los proveedores. Las normas armonizadas facilitarían la aplicación y la supervisión por parte de las autoridades reguladoras, tanto a escala nacional como de la UE. También garantizarían un mismo nivel de protección para todos los menores en internet en toda la UE, independientemente de los contextos socioeconómicos, culturales y nacionales.

RECOMENDACIÓN N.º 2

Introducir sistemas eficaces de garantía de la edad para comprobar la edad y respaldar la seguridad desde el diseño y enfoques adecuados a la edad para proteger y empoderar a los menores en línea

Los métodos de control de la edad —tanto la verificación como la estimación— deben ser proporcionados y respetar unos requisitos mínimos, en particular en lo que respecta a los derechos fundamentales de los usuarios, incluidos los derechos de los menores y las garantías conexas. Cualquier método empleado para comprobar la edad debe respetar las normas más estrictas en materia de privacidad y protección de datos, y no debe implicar el tratamiento de los documentos de identidad ni de los datos biométricos con el fin de estimar la edad. Deben implantarse normas técnicas, como la «prueba de conocimiento cero», a fin de garantizar que ni la plataforma encargada de evaluar la edad ni el proveedor de verificación de la edad reciban información alguna que permita rastrear o identificar al usuario.

Los métodos de control de la edad deben determinar con precisión la edad o los grupos de edad requeridos, y ser fáciles y fiables en la práctica, en condiciones reales. Los métodos deben ser sólidos para evitar su elusión y las amenazas a la ciberseguridad, inclusivos (y no discriminatorios) y estar disponibles por igual para todas las personas que necesiten utilizarlos. Los proveedores de medios sociales y otros servicios digitales deben cumplir su obligación de evitar que los menores se vean expuestos a servicios de riesgo y que haya usuarios que se hagan pasar por niños y adolescentes.

Para aplicar en la práctica una restricción de edad armonizada a escala de la UE, los proveedores tendrán que poder basarse en orientaciones y criterios claros sobre el uso de tecnologías de control de la edad con el fin de aplicar dichas restricciones. Además, los usuarios y los proveedores deberán poder acceder

a tecnologías de verificación de la edad eficaces, respetuosas de la privacidad, seguras, inclusivas y fáciles de usar para aplicarlas en la práctica. En este contexto, las soluciones de la UE para la verificación de la edad, basadas en el plan director de verificación de la edad de la UE, podrían proporcionar una herramienta armonizada, respetuosa de la privacidad, de vanguardia e interoperable para el cumplimiento de dichas obligaciones a escala de la UE.

Para reforzar aún más este marco, los Estados miembros, así como los agentes del mercado, deben poner a disposición herramientas operativas de verificación de la edad que se ajusten al plan director de verificación de la edad de la UE o se basen en él, y seguir la Recomendación de la Comisión sobre el establecimiento de un marco común para las tecnologías de verificación de la edad a escala de la UE. La Recomendación de la Comisión establece un sistema que definirá los requisitos relativos al modelo de confianza, la gobernanza y las obligaciones de los proveedores de soluciones para la verificación de la edad y declaraciones de prueba de la edad.

Los Estados miembros deben designar sin demora a proveedores de prueba de la edad de confianza. Para una verificación eficaz de la edad de los menores, también tendrán que garantizar que se faciliten o reconozcan las credenciales de edad para menores de 18 años. Esto incluiría garantizar que todos los menores puedan acceder a algún medio para demostrar su edad, incluso sin un documento nacional de identidad.

Es importante que la UE establezca una base jurídica clara para la aplicación de soluciones de verificación de la edad, a fin de garantizar que los proveedores de medios sociales y otros servicios digitales acepten a los proveedores de confianza de declaraciones de prueba de la edad. El control de la edad es fundamental para el buen funcionamiento de los sistemas de reclamaciones que empoderan a los niños y adolescentes para ejercer sus derechos y navegar de forma segura en línea.

RECOMENDACIÓN N.º 3

Ampliar y armonizar las normas sobre las características clave de seguridad en el diseño de las redes sociales y otros servicios digitales

Los medios sociales y otros servicios digitales deberían incorporar salvaguardias claras de seguridad desde el diseño y adecuadas a la edad (por ejemplo, posibles límites al *scroll* infinito, a la reproducción automática, a las notificaciones automáticas y a los motores de recomendación personalizados problemáticos). Para hacer frente al diseño que genera adicción, los patrones oscuros, el contacto no solicitado y las espirales de contenido, los ajustes predeterminados de protección deberían ser parte integrante de los medios sociales y otros servicios digitales. La ampliación y armonización de las normas sobre los elementos clave de seguridad garantizaría la seguridad y la uniformidad en todo el entorno de las redes sociales+. Debido al rápido desarrollo de la tecnología, cualquier norma sobre características clave de seguridad debería ser adaptable para poder abordar en permanencia nuevas características nocivas de diseño.

RECOMENDACIÓN N.º 4**Trasladar la carga de la prueba a los proveedores de medios sociales y otros servicios digitales para demostrar que sus productos y servicios son seguros para los menores**

Deberían aplicarse restricciones específicas de edad hasta que los proveedores de medios sociales y otros servicios digitales introduzcan elementos clave de diseño de seguridad que protejan a los niños y adolescentes. Hasta que los proveedores no demuestren haber incorporado elementos seguros y adecuados a la edad, cumpliendo así las medidas nacionales y de la UE, no deberían tener acceso a los menores. Cuando exista una versión «segura por defecto», los elementos inadecuados para la edad (elementos para adultos) solo deberían activarse tras unos controles de la edad eficaces.

RECOMENDACIÓN N.º 5**Reforzar las capacidades de ejecución y evaluación**

Habida cuenta de las múltiples normas que se aplican actualmente a la seguridad infantil en internet (el Reglamento de Servicios Digitales, el Reglamento General de Protección de Datos, el Reglamento de Inteligencia Artificial, etc.), las autoridades de control deberían intensificar la cooperación y el intercambio de información entre los marcos jurídicos. Esto es fundamental para evitar incoherencias y garantizar un entorno jurídico coherente, predecible y eficaz basado en la protección de los derechos fundamentales. La Comisión Europea debería explorar mecanismos que permitan una cooperación fluida entre las autoridades de supervisión para aprovechar las estructuras de ejecución existentes. Además, es necesario valorar si se necesitan recursos adicionales y reestructuración para las autoridades reguladoras responsables de la aplicación y la evaluación. Deberían considerarse actuaciones para reforzar el papel de la sociedad civil en la ejecución y su contribución a la capacidad de ejecución, también a través de las estructuras existentes. La ejecución debería ser complementaria y evitar actuaciones contradictorias.

RECOMENDACIÓN N.º 6**Adoptar rápidamente medidas para garantizar que los proveedores de medios sociales y otros de servicios digitales tengan obligaciones claras para prevenir, detectar, denunciar y bloquear el abuso sexual de menores en línea, también en las comunicaciones interpersonales**

Debería colmarse rápidamente la laguna en materia de seguridad infantil que existe actualmente debido a la expiración del Reglamento provisional por el que se establecen normas para prevenir y combatir el abuso sexual de menores. Los legisladores de la UE deberían adoptar rápidamente la propuesta de Reglamento para el largo plazo destinado a prevenir y combatir el abuso sexual de menores. Más del 80 % de las investigaciones de abuso sexual de menores parten de denuncias presentadas por los proveedores de medios sociales y otros servicios digitales. A menudo, los menores tienen demasiado miedo a denunciar abusos. Detectar material de abuso sexual de menores, también en las comunicaciones interpersonales, es a menudo la única manera de detenerlo.

Junto con la refundición de la Directiva sobre el abuso sexual de menores, acordada recientemente por los legisladores, estos instrumentos reforzarán el marco de la UE contra el abuso y la explotación

sexuales de menores, tanto en línea como fuera de línea. Mejorarán la prevención, la investigación y el apoyo a las víctimas. Además, las plataformas en línea deben reforzar la cooperación intrasectorial en materia de delitos graves en línea que afectan a los niños, compartiendo señales sobre contenidos nocivos y agentes malintencionados. Los proveedores de medios sociales y otros servicios digitales deben reforzar la cooperación con el Foro de la UE sobre Internet para compartir información sobre amenazas emergentes y patrones de abuso. Esto facilitará la detección precoz y la denuncia de presuntas infracciones penales. Además, es necesario intensificar la aplicación de los marcos jurídicos de protección de la infancia, como la Directiva sobre los derechos de las víctimas o la Directiva sobre la violencia contra las mujeres y la violencia doméstica.

RECOMENDACIÓN N.º 7

Los Estados miembros pueden introducir restricciones preventivas adicionales de acceso a las redes sociales y otros servicios digitales a partir de los 13 años

Las restricciones prudenciales adicionales de acceso deben ser complementarias a la restricción de acceso a los medios sociales y otros servicios digitales a escala de la UE contemplada en el punto 13. Los adolescentes solo pueden tener acceso a un entorno de medios sociales+ que sea seguro, tanto en contenidos como en las características de diseño, adecuado a la edad y diseñado teniendo en cuenta sus derechos y necesidades. Los Estados miembros tienen diversos contextos históricos y nacionales diversos y pueden preferir fijar un umbral de edad superior a los 13 años. Todas las restricciones nacionales de acceso prudenciales adicionales deberían estar sujetas a una evaluación continua y, en su caso, reevaluarse, una vez que los medios sociales y otros servicios digitales sean seguros por defecto para niños y adolescentes.

RECOMENDACIÓN N.º 8

Reforzar las políticas de protección de los consumidores para proteger a los niños

La legislación en materia de protección de los consumidores desempeña un papel importante como instrumento de protección de la infancia, ya que abarca a todos los tipos de operadores comerciales (tiendas en línea de comercio electrónico, servicios de emisión en continuo y contenidos digitales basados en suscripciones, videojuegos y aplicaciones) y garantiza que ningún operador comercial que interactúe con menores quede fuera del ámbito de aplicación de las obligaciones exigibles en materia de protección de los consumidores. Debe reforzarse la protección de los niños frente a las prácticas de comercialización en línea engañosas, agresivas y perjudiciales, también por parte de influyentes en línea.

La red de seguridad y las normas que rigen su aplicación deben reforzarse para garantizar que todos los menores que interactúen con un servicio digital comercial en la Unión Europea se beneficien de un nivel básico de protección de los consumidores, independientemente del tipo de servicio, del tipo de operador comercial o del Estado miembro en el que esté establecido el operador.

La próxima Ley de Equidad Digital y la revisión del Reglamento sobre la cooperación en materia de protección de los consumidores (CPC) constituyen una oportunidad clave para situar la protección de los niños y adolescentes en el centro de la legislación de la UE en materia de protección de los consumidores.

RECOMENDACIÓN N.º 9**Supervisar y evaluar continuamente el impacto de las medidas que se están aplicando**

Todos los nuevos instrumentos propuestos a raíz de las recomendaciones de este capítulo deben incluir mecanismos y enfoques basados en datos para evaluar continuamente su impacto y eficacia. La Comisión también debe mejorar la coordinación de los esfuerzos de ejecución y la racionalización de los procesos de evaluación y seguimiento relativos específicamente a la seguridad infantil en línea.

Sobre la base del modelo aplicado para hacer un seguimiento de la aplicación de la legislación australiana en materia de medios sociales (incluida la integración continua de los conocimientos y las aportaciones de los expertos), el establecimiento de una restricción de acceso a escala de la UE debe ir acompañado de una evaluación exhaustiva. Debe centrarse en la eficacia, las repercusiones y las adaptaciones del régimen de edad mínima, dando prioridad a la participación de los niños. Esto podría lograrse utilizando los mecanismos existentes, como la Plataforma de Participación Infantil de la UE y «Una Internet mejor para los niños» (BIK+), y racionalizando la investigación sobre esta cuestión en toda la UE y en diferentes ámbitos de estudio, incluidos los programas de investigación estructurados.

Estas evaluaciones pueden basarse en el trabajo en curso en el marco del Reglamento de Servicios Digitales y del Centro Europeo para la Transparencia Algorítmica (ECAT). El Centro supervisa continuamente cómo evoluciona el panorama de la seguridad infantil en línea en lo que respecta a las tendencias en desarrollo, las posibilidades y el uso de tecnologías nuevas y emergentes. Esto puede servir de base para establecer un sistema de recogida de datos estructurada y periódica a partir de muestras representativas de menores de las cohortes de edad pertinentes en toda la UE.

El objetivo principal de la evaluación es el bienestar de los menores. Los marcos de evaluación deben incluir resultados relacionados con el desarrollo, indicadores de salud mental, medidas de bienestar y resultados en materia de resiliencia, en lugar de centrarse exclusivamente en parámetros de cumplimiento, exposición o uso. En última instancia, las políticas de seguridad infantil deben evaluarse en función de su contribución a un desarrollo saludable.

RECOMENDACIÓN N.º 10**Al tratar los datos de los menores en virtud del RGPD, las redes sociales y otros servicios digitales deben garantizar que el interés superior del menor sea una consideración primordial**

Cuando los medios sociales y otros servicios digitales, como responsables o encargados del tratamiento, traten datos personales de menores, deben asegurarse de que se basan en el fundamento jurídico más adecuado en virtud del RGPD. Las autoridades de protección de datos evalúan si los responsables del tratamiento tratan los datos de menores con arreglo a una base jurídica adecuada y si se cumplen las condiciones pertinentes.

Si un responsable del tratamiento opta por tratar los datos personales de un menor sobre la base del consentimiento, debe asegurarse de haber obtenido el consentimiento válido del menor y, en caso necesario, el consentimiento del titular de la responsabilidad parental.

Si un responsable del tratamiento opta por basarse en el interés legítimo como fundamento jurídico para el tratamiento de los datos personales de los niños, debe garantizar que se cumplen todos los requisitos del artículo 6, apartado 1, letra f), antes de llevar a cabo el tratamiento. Uno de estos requisitos es que los intereses legítimos de los responsables del tratamiento no prevalezcan sobre los intereses o los derechos y libertades fundamentales del interesado. A este respecto, debe prestarse especial atención cuando el interesado sea un niño.

Como se señala en las directrices del Comité Europeo de Protección de Datos (CEPD) sobre el interés legítimo, al llevar a cabo esta evaluación, los responsables del tratamiento deben tener en cuenta el alcance y la intensidad de cualquier injerencia en los derechos y libertades del menor. Deben tener en cuenta las expectativas razonables del menor en cuanto al uso que se hará de sus datos personales. Además, deben demostrar que el interés superior del menor se ha tenido en cuenta como consideración primordial y que existen las salvaguardias adecuadas. El interés superior del menor debe ser una consideración primordial a la hora de sopesar los intereses contrapuestos en juego.

Cuando los intereses legítimos del responsable del tratamiento entren en conflicto con los intereses o los derechos y libertades fundamentales de un menor, los intereses y derechos de este último deben prevalecer, por regla general. Si esto no puede garantizarse, el responsable del tratamiento debe buscar una base jurídica más adecuada o abstenerse de tratar los datos personales del menor.

RECOMENDACIÓN N.º 11

Garantizar la aplicación efectiva de la Directiva sobre responsabilidad por los daños causados por productos defectuosos

Adoptada originalmente en 1985, la Directiva se actualizó durante el último mandato de la Comisión Europea para reflejar importantes avances tecnológicos, económicos y jurisprudenciales. El objetivo era garantizar la igualdad de condiciones, aportando seguridad jurídica a las empresas y garantizando al mismo tiempo una reparación efectiva a las víctimas. La Directiva revisada entró en vigor el 8 de diciembre de 2024 y los Estados miembros deben transponerla a más tardar el 9 de diciembre de 2026.

Teniendo en cuenta la evolución de los casos de responsabilidad por los daños causados por productos defectuosos contra los servicios digitales en todo el mundo, es fundamental garantizar la transposición y aplicación efectivas y oportunas de la Directiva. Además, los reguladores deben dar a conocer de manera eficaz a los ciudadanos los derechos derivados de la Directiva sobre responsabilidad por los daños causados por productos defectuosos (por ejemplo, promoviendo los mecanismos de recurso actualizados para las personas que deseen interponer una demanda por el uso de un producto defectuoso, especialmente en el caso de los programas informáticos).

04

Capacitar a los menores para navegar con seguridad por el mundo digital

En el capítulo anterior se examinaron la legislación vigente y las herramientas existentes de que disponen la UE y los Estados miembros para proteger a los menores en línea, se presentaron los resultados de las medidas de aplicación en curso y se identificaron ámbitos en los que es necesario reforzar y completar la legislación y las herramientas para mejorar la seguridad de los menores en línea.

Sin embargo, el mundo de los medios sociales+ no puede reducirse únicamente a los riesgos. También es un espacio de oportunidades para la creatividad y la participación. En este capítulo se analizan las pruebas, aunque limitadas en comparación, relativas a las oportunidades que ofrece el uso de los medios sociales y otros servicios digitales por parte de los menores. Tiene en cuenta las contribuciones de una representante de la juventud, Marta Gonçalves, que participó en las reuniones del panel especial y en los debates que condujeron a la formulación de las recomendaciones de los copresidentes.

Este capítulo continúa con la revisión de determinadas políticas y herramientas de la UE que promueven el empoderamiento y la participación de los menores en línea. Termina con una serie de recomendaciones sobre cómo ayudar a los niños y a sus círculos de apoyo (progenitores, cuidadores, profesores y educadores) a aprovechar las oportunidades que ofrece el mundo en línea.

Este capítulo se basa en los pilares quinto y sexto de los seis principios rectores presentados por los copresidentes para orientar los esfuerzos destinados a reforzar la seguridad infantil en línea: empoderamiento y educación mediática, y derechos y participación de los niños. Este análisis toma como punto de partida los respectivos marcos internacionales y de la UE sobre los derechos del niño^a.

Para ser eficaces, las medidas de protección de la infancia en línea deben ir acompañadas de acciones que promuevan el empoderamiento y la participación de los menores. Las medidas deben ser adecuadas a la edad, teniendo en cuenta la evolución de las capacidades de los niños y adolescentes, y adaptarse a las funciones cambiantes de los cuidadores y educadores a lo largo de la trayectoria de los menores hacia la edad adulta.

a. En particular, la Convención de las Naciones Unidas sobre los Derechos del Niño y las Observaciones generales del Comité de los Derechos del Niño, la Carta de los Derechos Fundamentales de la Unión Europea y la Estrategia de la UE sobre los Derechos del Niño.

Más allá de los riesgos, debe reconocerse que el mundo digital también ofrece a los niños y adolescentes muchas oportunidades. Cuando los menores están capacitados para interactuar de forma segura en línea y tienen competencias digitales sólidas, el uso de los medios sociales y otros servicios digitales puede favorecer el bienestar, la conexión social, proporcionar redes de apoyo entre iguales, oportunidades para la autoexpresión, el compromiso cívico y el aprendizaje independiente.

En la siguiente sección se examinan las posibles oportunidades relacionadas con el uso de los medios sociales+ por parte de niños y adolescentes. Pero, antes de nada, este capítulo da la palabra a una representante de la juventud.

Configurar un mundo digital mejor

UN LLAMAMIENTO A LA ACCIÓN DE MARTA GONÇALVES,

EMBAJADORA DE PORTUGAL PARA «UNA INTERNET MEJOR

PARA LOS NIÑOS»

«Crecí en un mundo en el que internet nunca estuvo separada de la vida cotidiana. Para mi generación, estar conectado no es una actividad ocasional. El espacio digital es donde aprendemos, creamos, nos comunicamos, entablamos amistades, descubrimos oportunidades y desarrollamos nuestras identidades. Esta es la razón por la que empoderar a los niños y los jóvenes para que utilicen los medios sociales y otras tecnologías digitales de forma segura no consiste simplemente en protegerlos de los daños. Se trata de permitirles participar plenamente en el mundo en el que crecen.

Con demasiada frecuencia, los debates sobre la vida digital de los niños se producen sin que ellos mismos participen. Los Gobiernos, las empresas, los educadores y los adultos toman decisiones en nombre de los jóvenes y rara vez preguntan a los más afectados qué necesitan realmente. Esto no solo es injusto, sino también contraproducente. No podemos construir mejores entornos digitales basándonos en conjeturas sobre las experiencias de los niños.

A través de mi propio trabajo de asesoramiento entre iguales y representación juvenil, he sido testigo del increíble potencial de los jóvenes cuando se confía en ellos y se les atribuye responsabilidad. Los niños y adolescentes pueden lograr cosas extraordinarias gracias a su creatividad, empatía, determinación y voluntad de ayudarse mutuamente. Cuando los jóvenes se reúnen, no se limitan a consumir tecnología. La utilizan para aprender, crear, resolver problemas y crear comunidades. Se convierten en modelos a seguir para sus compañeros de una forma que los adultos no pueden igualar.

Los jóvenes son expertos en sus propias realidades. Saben qué oportunidades valoran, los retos a los que se enfrentan y las soluciones que realmente marcarían la diferencia. La participación significativa de los jóvenes no debe tratarse como un ejercicio simbólico, sino que debe reconocerse como una parte esencial del diseño de políticas, plataformas y servicios digitales que realmente funcionen.

El proceso del panel especial ofreció un ejemplo contundente de cómo puede ser la participación significativa de los jóvenes. A lo largo de las tres reuniones, los representantes de los niños y jóvenes se integraron plenamente en los debates, participando junto con otros expertos, aportando sus perspectivas y compartiendo las preocupaciones que más les importaban.

Además, también tuve la oportunidad de participar en la elaboración del propio informe, redactar secciones y aportar ideas a lo largo de todo el proceso de elaboración de las recomendaciones. No solo me consultaron, sino que me integraron de manera significativa en el proceso y contribuí con mis conocimientos y experiencia, tal como se refleja en este capítulo (véase, por ejemplo, la sección sobre el asesoramiento entre iguales). La participación en los debates en los que se configuraron las decisiones, el intercambio de argumentos, la escucha de diferentes perspectivas y la obtención de nuevos conocimientos reforzaron el valor de la participación de los jóvenes a lo largo de todo el proceso y del reconocimiento de sus experiencias vividas como fuente de conocimiento.

Aunque el panel especial se centró en desarrollar un enfoque para garantizar la seguridad de los niños en línea, me comprometí igualmente a contribuir a poner de relieve las oportunidades que ofrece el mundo digital.

El mundo en línea ha abierto puertas que las generaciones anteriores apenas podían imaginar. Permite a los niños aprender nuevas lenguas, tocar instrumentos musicales, descubrir temas científicos, desarrollar competencias artísticas, explorar nuevas culturas y conectar con personas que comparten sus pasiones, independientemente de su ubicación geográfica. Para muchos jóvenes, especialmente aquellos que pueden sentirse aislados en sus comunidades locales, los espacios digitales se convierten en lugares en los que encuentran un sentido de pertenencia, inspiración y confianza. Internet puede crear oportunidades que marquen el rumbo de nuestras vidas, pero solo si los niños cuentan con los conocimientos y el apoyo necesarios para navegar por ella de forma segura.

La experiencia también me ha enseñado que los niños informados son niños empoderados. Cuando los jóvenes entienden cómo funcionan las plataformas digitales, cómo proteger su privacidad, cómo identificar la manipulación, la desinformación o los comportamientos nocivos, ganan confianza a la hora de reconocer cuándo algo no va bien. Están mejor preparados para buscar ayuda, apoyar a sus amigos y contribuir a que las comunidades en línea sean más seguras. La alfabetización digital no consiste en enseñar a los niños a temer a las tecnologías. Se trata de dotarles de la confianza y los conocimientos necesarios para utilizarlas de manera crítica, responsable y positiva.

El conocimiento es una de las herramientas más poderosas que podemos dar a un niño. La información permite tomar decisiones con conocimiento de causa, aumenta la resiliencia y genera independencia. Todos los niños merecen tener acceso a una orientación clara y adecuada a su edad que les ayude a comprender tanto las oportunidades como los riesgos del mundo digital. Cuanto más invirtamos en educación, participación y alfabetización digital, más empoderaremos a los jóvenes para que se protejan a sí mismos y a los demás en línea.

El futuro del mundo digital lo forjarán los niños de hoy. No son simplemente futuros ciudadanos, sino que ya son participantes activos cuyas voces, ideas y experiencias importan. Si los empoderamos hoy, no solo podrán desenvolverse en el mundo digital, sino que lo redefinirán para mejor».



Marta Gonçalves

Embajadora de Portugal para «Una Internet mejor para los niños»

Marta Gonçalves

Oportunidades para los menores en el mundo digital

CONEXIÓN Y AUTOEXPRESIÓN

«Existe una necesidad apremiante de adoptar un enfoque basado en la autonomía con respecto a los jóvenes. Los niños se ven limitados por todas partes por unos progenitores ansiosos y los medios sociales son un escape de esa situación. Los jóvenes deben participar en las decisiones y en el debate sobre los espacios en línea, ya que solo así cumplirán la normativa y se les empoderará, a través de la resiliencia, para desarrollar una recepción crítica y competencias de autogestión de cara a un futuro digital impredecible.»

— ZUZANNA,
REPRESENTANTE DE 17 AÑOS DE LA
PLATAFORMA DE PARTICIPACIÓN INFANTIL
DE LA UE

Como ya se ha mencionado en el capítulo 2, muchos niños y adolescentes utilizan los medios sociales+ para conectarse, interactuar y compartir sus intereses con otras personas en línea, y las pruebas ponen de relieve estas conclusiones²⁹⁰.

Los medios sociales+ también pueden permitir a los adolescentes compartir sus intereses con sus compañeros en línea, cultivar amistades iniciadas fuera de línea y mantenerse en contacto con amigos cercanos y familiares que viven lejos²⁹¹.

En términos más generales, el uso de los medios sociales y otros servicios digitales puede permitir a los adolescentes entretenerse juntos y reflexionar sobre experiencias comunes en línea, y las investigaciones apuntan a posibles beneficios para el estado de ánimo y el bienestar de los adolescentes²⁹².

Los medios sociales+ también pueden proporcionar espacios para que los adolescentes se expresen y exploren su identidad²⁹³. Las investigaciones sugieren que los espacios en línea pueden ofrecer entornos percibidos como «menos arriesgados» para la revelación selectiva de información personal²⁹⁴. Además, algunos menores pueden utilizar cuentas privadas en medios sociales de manera similar a los diarios personales fuera de línea²⁹⁵.

Los adolescentes utilizan cada vez más los medios sociales+, en particular como vía de expresión creativa. Una encuesta realizada en 2022 a 1 316 adolescentes estadounidenses reveló que el 71 % consideraba los medios sociales como un espacio para expresar su creatividad²⁹⁶. Sin embargo, estos usos pueden exponer a los adolescentes a daños.

En resumen, los posibles beneficios del uso de los medios sociales y otros servicios digitales por parte de los menores para la conexión y la autoexpresión deben ser sopesados por sus círculos de apoyo frente a los riesgos para la seguridad, la salud y el bienestar de los niños y adolescentes. Esto

incluye los riesgos de contacto no deseado y de exposición a contenidos en línea inadecuados para su edad, en particular la captación y el abuso sexuales de menores.

Mantener conversaciones abiertas con los menores sobre sus experiencias en línea es fundamental para garantizar que los niños y adolescentes se sientan cómodos a la hora de informar a sus progenitores o cuidadores, en particular, de contactos o experiencias no deseados. Además, los cuidadores y educadores deben estar dotados de las competencias necesarias para supervisar (y, en caso necesario, restringir) el uso de los medios sociales+ por parte de los menores, así como para saber a quién acudir para obtener ayuda profesional cuando sea necesario.

APOYO E INFORMACIÓN

Muchos adolescentes utilizan los medios sociales y otros servicios digitales para buscar apoyo ante los problemas que experimentan en línea. Algunas investigaciones sugieren que el uso de los medios sociales+ por parte de los adolescentes puede fomentar conversaciones abiertas y permitirles encontrar ayuda en línea²⁹⁷.

Una idea que suelen expresar los menores es que los espacios en línea ofrecen alternativas «seguras» para la autoexpresión o fuentes de apoyo más accesibles en comparación con las opciones «tradicionales», como hablar con los progenitores o los orientadores²⁹⁸.

Tal como se analiza en el capítulo 2, los adolescentes con buena autoestima y amistades fuera de línea pueden llegar a reforzar sus relaciones fuera de línea y encontrar apoyo en línea. Sin embargo, en el caso de aquellos con menor autoestima y redes sociales más débiles fuera de línea, los entornos de los medios sociales+ pueden aumentar la exposición de los adolescentes a contactos no deseados y a contenidos inadecuados para su edad.

Los menores vulnerables, incluidos los pertenecientes a comunidades LGBTIQ+, con necesidades educativas especiales, que sufren problemas de salud mental, trastornos alimentarios o se autolesionan, pueden mostrarse especialmente inclinados a utilizar los medios sociales y otros servicios digitales para conectar con otras personas que tengan experiencias similares o buscar apoyo.

Las escasas investigaciones disponibles indican que algunos adolescentes pueden encontrar consuelo respecto a los problemas que experimentan no solo a través de la interacción directa en línea, sino también al saber que otras personas están pasando por experiencias similares²⁹⁹.

Sin embargo, el uso de los medios sociales+ por parte de los menores para buscar apoyo puede exponer a personas ya vulnerables a daños, como el ciberacoso y la exclusión social, con posibles consecuencias negativas para su salud y bienestar.

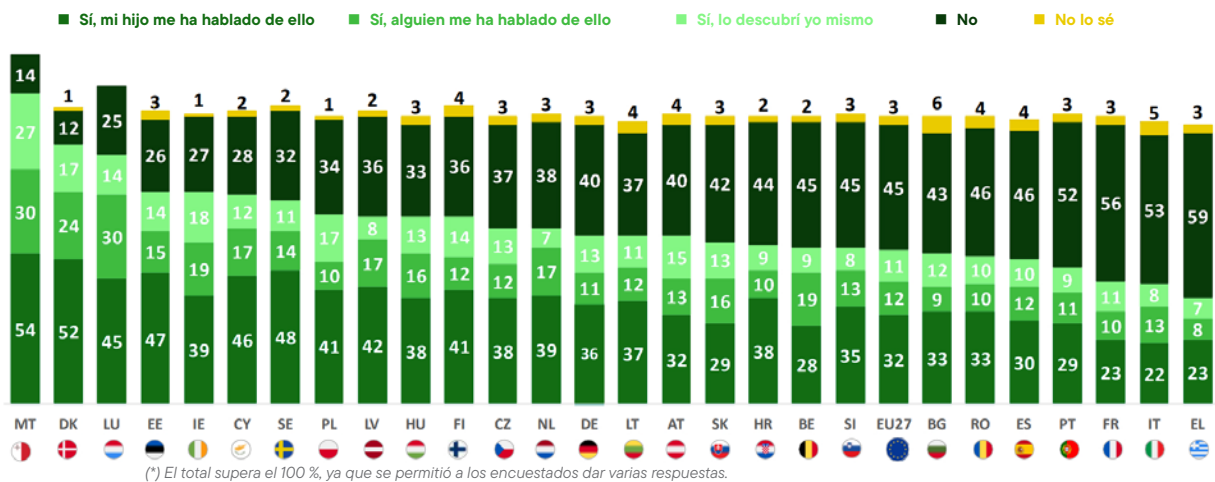
Con las salvaguardias adecuadas, los espacios de los medios sociales+ pueden ofrecer apoyo a los menores. Los foros de debate en línea gestionados y moderados por profesionales sanitarios, por ejemplo, podrían ofrecer una alternativa a quienes buscan ayuda o información en las plataformas de medios sociales+.

Algunas pruebas indican que la participación en este tipo de foros puede ayudar a los adolescentes a superar sus reticencias a la hora de buscar ayuda profesional a través de los canales «tradicionales»³⁰⁰. Esto también podría ayudar a abordar los problemas relacionados con la difusión de desinformación e información errónea en línea, por ejemplo, en lo que respecta a cuestiones médicas.

Los cuidadores, educadores y servicios públicos (incluidos los profesionales de la salud mental y la salud sexual) deben reflexionar sobre la mejor manera de informar y apoyar a los menores para que utilicen de forma segura los medios sociales y otros servicios digitales como fuente de información o apoyo.

Gráfico 1: Concienciación de las familias sobre las experiencias negativas de los menores en línea

Pregunta: ¿Alguna vez le ha contado su hijo o ha descubierto usted mismo que ha tenido una experiencia negativa en línea?



Fuente: Comisión Europea (2026). Encuesta del Eurobarómetro sobre el impacto del tiempo excesivo frente a las pantallas y de los medios sociales en la salud mental de los jóvenes, junio de 2026.

APRENDIZAJE Y DESARROLLO DE COMPETENCIAS

Los estudios sobre el uso de herramientas digitales para el aprendizaje sugieren que el uso de herramientas y servicios digitales puede tener un efecto positivo de leve a moderado en los resultados académicos de los niños en la enseñanza secundaria³⁰¹.

Las tecnologías digitales ofrecen a profesores y alumnos oportunidades adicionales para la enseñanza y el aprendizaje y parecen ser más eficaces cuando se utilizan para complementar, en lugar de sustituir, la enseñanza tradicional³⁰².

En materias como la ciencia, las matemáticas y las lenguas, las tecnologías digitales pueden enriquecer el aprendizaje a través de experiencias interactivas. Esto incluye simulaciones, modelización, animaciones, juegos digitales, recursos multimedia y efectos sonoros. Estos enfoques pueden aumentar la participación de los alumnos y ayudar a que los conceptos abstractos o complejos resulten más accesibles y comprensibles³⁰³.

Las herramientas y servicios digitales también pueden favorecer el aprendizaje personalizado. Al permitir a los alumnos avanzar a su propio ritmo y explorar temas desde diferentes ángulos, aportan una mayor flexibilidad en el proceso de aprendizaje. Esto puede aumentar la motivación, en particular en el caso de los alumnos que se benefician de la práctica repetida o de la investigación autodirigida³⁰⁴.

Las tecnologías basadas en la IA son una herramienta adicional que puede facilitar la enseñanza individualizada. Estas herramientas ofrecen a los profesores la oportunidad de adaptar los métodos en función del rendimiento de los alumnos, proporcionar comentarios y ajustes oportunos y ofrecer un apoyo personalizado en consecuencia³⁰⁵.

Las investigaciones indican que el uso de la IA generativa se ha integrado en las rutinas académicas de muchos alumnos³⁰⁶. Si bien los alumnos reconocen los riesgos para su aprendizaje y desarrollo cognitivo, tienden a centrarse en las posibles oportunidades³⁰⁷, por ejemplo, el ahorro de tiempo que supone el uso de una herramienta de IA.

El uso de plataformas de aprendizaje en las escuelas puede permitir a los alumnos de primaria y secundaria acceder a una mayor variedad de recursos de aprendizaje de calidad, lo que facilita el aprendizaje independiente, así como la posibilidad de autoevaluación y de evaluación por parte de sus compañeros³⁰⁸.

Estas oportunidades deben sopesarse con los riesgos, incluido el potencial de los dispositivos digitales para distraer a los niños y adolescentes del aprendizaje, los riesgos físicos (por ejemplo, en lo que respecta a la vista de los menores) y la «sobre digitalización» de la educación.

El impacto de las herramientas de IA en la educación y el desarrollo de competencias de los niños y adolescentes debe analizarse más a fondo para comprender los posibles beneficios y riesgos, tal como se explica en el capítulo 2. Del mismo modo, se necesitan más pruebas sobre los posibles efectos positivos del uso de los medios sociales+ en entornos educativos.

La educación digital, incluida la alfabetización mediática y en materia de IA, es fundamental para capacitar a los niños y adolescentes para navegar por el mundo en línea de forma segura. La cuestión principal es cómo integrar de manera práctica la adquisición de competencias y alfabetización digitales en los planes de estudios, de forma que resulte beneficiosa para el aprendizaje y el desarrollo generales de los menores.

«Los jóvenes necesitan derechos claros, información comprensible, herramientas de denuncia eficaces y una voz real a la hora de configurar los espacios digitales que utilizan a diario. Internet no es solo un lugar de riesgo. Para muchos jóvenes, también es un lugar de aprendizaje, conexión, creatividad y apoyo. Así pues, en lugar de prohibir o restringir, convirtámosla en un lugar de inspiración, seguro para todos. Por eso mi mensaje es sencillo: hay que construir internet con nosotros, no solo para nosotros.»

— AYATA,
REPRESENTANTE DE 15 AÑOS DE LA
PLATAFORMA DE PARTICIPACIÓN INFANTIL
DE LA UE

Las culturas y actitudes respecto al uso de dispositivos y herramientas digitales en entornos de aprendizaje varían considerablemente a escala nacional en toda la UE. Sin embargo, existe un amplio reconocimiento de la importancia de mejorar las competencias de los menores, los cuidadores y los educadores, de proporcionar herramientas de aprendizaje seguras y adecuadas a la edad, y de la necesidad de integrar el concepto de bienestar digital en las escuelas.

RESTRICCIONES AL USO DE TELÉFONOS INTELIGENTES EN LAS ESCUELAS

Los teléfonos móviles se han convertido en algo omnipresente en la vida de niños y adolescentes de toda Europa. Tal como se analiza en el capítulo 1, el uso de teléfonos inteligentes por parte de los menores en la escuela puede distraerlos del aprendizaje, poner en peligro su rendimiento académico, reducir la interacción social y, al mismo tiempo, aumentar el riesgo de sufrir daños, como el ciberacoso y la exclusión social.

En el caso de los adolescentes, el uso de teléfonos inteligentes puede aumentar el riesgo de sufrir problemas de salud mental, como la ansiedad y la depresión. En términos más generales, el uso de teléfonos inteligentes por parte de los menores en el aula puede someter a los profesores a una «ansiedad por la vigilancia» y a un estrés adicional relacionado con la necesidad de controlar el uso de los dispositivos.

Estos riesgos detectados han suscitado debates en los Estados miembros de la UE y fuera de ella sobre si se debe prohibir el uso de teléfonos inteligentes por parte de niños y adolescentes en la escuela. Las medidas propuestas van desde prohibiciones totales durante el horario escolar hasta políticas de restricción más matizadas que implican un uso condicional o supervisado.

A finales de 2025, la mayoría de los Estados miembros de la UE había aplicado, o tenía previsto aplicar, alguna forma de restricción de los teléfonos móviles en las escuelas. Las medidas van desde prohibiciones totales durante la jornada escolar (Austria, Bélgica, Chipre, Francia, Hungría, Portugal y Eslovenia), que a menudo implican la recogida obligatoria de dispositivos, hasta restricciones limitadas al aula que dejan las medidas más amplias a la discreción de la escuela (Países Bajos, Rumanía y Eslovaquia). Algunos países (Bulgaria y Suecia) están pasando de marcos de carácter orientativo a normas jurídicamente vinculantes.

Las prohibiciones durante toda la jornada son la solución más habitual, pero su aplicación varía (por ejemplo, en Suecia hubo un 80 % de respuestas positivas, mientras que el 20 % tuvo dificultades para aplicar las prohibiciones)³⁰⁹.

Entre los retos detectados y las consecuencias no deseadas de las medidas restrictivas figuran la carga que supone para el personal no docente la recogida de dispositivos, los efectos de sustitución (los menores sustituyen el uso de teléfonos inteligentes, por ejemplo, por tabletas u ordenadores portátiles), el desplazamiento del ciberacoso a las horas extraescolares y la compensación excesiva del uso de teléfonos inteligentes por las tardes.

Políticas y herramientas de la UE

Tras examinar las oportunidades que ofrece el uso de los medios sociales y otros servicios digitales por parte de los niños y adolescentes, sopesándolas a la luz de los riesgos que estas actividades plantean para la salud y el bienestar de los menores, la siguiente sección presenta una selección de políticas y herramientas de la UE que promueven el empoderamiento y la participación de los menores en línea.

El análisis se centra en las políticas y herramientas que, a juicio de los copresidentes, pueden complementarse o completarse con otras medidas.

ESTRATEGIA DE LA UE SOBRE LOS DERECHOS DEL NIÑO

La Comisión Europea adoptó la Estrategia de la UE sobre los Derechos del Niño en 2021 como un marco político integral para defender los derechos de los niños en todas las políticas de la UE y garantizar que los niños vulnerables tengan un acceso seguro a los servicios básicos.

La Estrategia se estructura en torno a seis pilares:

1. participación de los niños en la vida política y democrática, incluida la Plataforma de Participación Infantil de la UE;
2. inclusión socioeconómica, salud y educación, incluida la Garantía Infantil Europea;
3. lucha contra la violencia ejercida contra los niños y garantía de la protección de la infancia;
4. justicia adaptada a los niños;
5. entorno digital;
6. dimensión mundial.

El pilar digital, que se comprometió a seguir apoyando los Centros de Seguridad en Internet y «Una Internet mejor para los niños», garantiza que los niños puedan disfrutar de entornos digitales seguros y de un acceso equitativo a las herramientas digitales.

La Estrategia invitó a los Estados miembros de la UE a garantizar un acceso equitativo y efectivo a las herramientas digitales, apoyar las acciones de alfabetización mediática a través de la educación, desarrollar la capacidad de los niños para evaluar críticamente los contenidos en línea y detectar la desinformación y el material abusivo.

Además, invita a los Estados miembros a promover y apoyar los Centros de Seguridad en Internet co-financiados por la UE, las líneas de ayuda a la infancia y las líneas directas de denuncia. Por último, la Estrategia invita a los Estados miembros de la UE a fomentar la participación de los niños (especialmente de las niñas) en la educación en ciencia, tecnología, ingeniería y matemáticas (CTIM).

En la Estrategia de la UE sobre los Derechos del Niño, la Comisión Europea invita a las empresas del sector de las TIC a:

- // garantizar que los derechos de los niños, incluida la privacidad, la protección de los datos personales y el acceso a contenidos adecuados a la edad, se incluyan en los productos y servicios digitales desde el diseño y por defecto, también los correspondientes a los niños con discapacidad;
- // dotar a los niños y a los progenitores de herramientas adecuadas para controlar su tiempo y comportamiento ante las pantallas, y protegerlos de los efectos del uso excesivo y la adicción a los productos en línea;
- // reforzar las medidas para ayudar a reaccionar ante los contenidos nocivos y las comunicaciones comerciales inadecuadas, por ejemplo, mediante canales de notificación y bloqueo fáciles de utilizar o herramientas eficaces de comprobación de la edad;
- // proseguir sus esfuerzos para detectar, denunciar y eliminar contenidos ilícitos en línea, como los abusos sexuales de menores, de sus plataformas y servicios, en la medida en que dichas prácticas sean legales.

UNA INTERNET MEJOR PARA LOS NIÑOS

La Comisión Europea colabora directamente con los niños, junto con expertos, progenitores, cuidadores, profesores y otras partes interesadas pertinentes, para garantizar que se tengan en cuenta diversas perspectivas en el desarrollo y la aplicación de las políticas relacionadas con el entorno digital.

La Estrategia para «Una Internet mejor para los niños» (BIK+) ofrece un marco integral destinado a proteger, empoderar y respetar a los menores en línea, incluidos los más vulnerables. La Estrategia apoya la aplicación de los instrumentos legislativos de la UE en este ámbito, complementando las obligaciones con medidas de sensibilización, desarrollo de capacidades y apoyo.

La plataforma «Una Internet mejor para los niños» ofrece una amplia colección de recursos educativos diseñados para ayudar a los niños y los jóvenes a desarrollar las competencias digitales necesarias para participar de forma segura, responsable y con confianza en entornos en línea.

La plataforma adopta un enfoque multilateral que ofrece rincones de aprendizaje específicos para niños, jóvenes, progenitores, cuidadores, profesores y educadores. Esto refleja el papel de los cuidadores y educadores, como parte de los círculos de apoyo de los niños y adolescentes, a la hora de supervisar y orientar el uso de los medios sociales y otros servicios digitales por parte de los menores.

Rincón de los Niños

El Rincón de los Niños de la plataforma «Una Internet mejor para los niños» está diseñado para capacitar a los niños y jóvenes para navegar por el mundo digital, proporcionando diversos materiales de aprendizaje interactivos y atractivos. Entre ellos se incluyen juegos educativos que refuerzan el conocimiento y la sensibilización sobre la seguridad infantil en línea, el comportamiento responsable en línea y la prevención del uso excesivo y el abuso de internet.

El Rincón de los Niños también ofrece material didáctico que presenta a los niños la labor de la UE y las oportunidades de participación ciudadana a través de iniciativas, como la Plataforma de Participación Infantil de la UE (que se analiza más adelante en este capítulo).

Rincón de los Progenitores

El Rincón de los Progenitores de la plataforma «Una Internet mejor para los niños» apoya a los progenitores, cuidadores y adultos responsables de niños, proporcionando orientación práctica y recursos educativos basados en datos contrastados sobre una serie de cuestiones relacionadas con las experiencias de los niños en línea.

Hay secciones específicas que abordan temas como las herramientas de supervisión parental, los juegos en línea y la gestión del tiempo frente a la pantalla. Además, la plataforma ofrece una serie de módulos de aprendizaje y sesiones de profundización destinados a reforzar la comprensión por parte de los progenitores tanto de los riesgos como de las oportunidades que presentan los medios sociales y las tecnologías digitales.

Los módulos de formación básica abarcan temas como la ciberseguridad, la lucha contra la violencia de género en línea, los juegos en línea, las prácticas de comercialización manipuladoras en los juegos, la comprensión de la información errónea y la desinformación, el sexteo, el ciberacoso y el papel de los progenitores a la hora de apoyar y educar a los niños en el mundo digital.

Cada módulo incluye contenido explicativo, actividades sugeridas y recursos complementarios para facilitar el aprendizaje autónomo.

Rincón del Profesor

Por último, el Rincón del Profesor ofrece a profesores, educadores y otros profesionales que trabajan con niños y jóvenes una serie de recursos educativos diseñados para mejorar su capacidad a la hora de abordar la seguridad infantil en línea y la ciudadanía digital en entornos educativos.

Los módulos de aprendizaje introductorios se centran en aspectos fundamentales de la seguridad infantil en línea y en las responsabilidades de los educadores a la hora de apoyar a los niños y jóvenes. Abordan temas como los principales riesgos para la seguridad en línea, la enseñanza de la alfabetización mediática y la ciudadanía digital en los centros de enseñanza primaria y secundaria, la aplicación de enfoques escolares integrales para la seguridad infantil en línea y los derechos de los niños en el mundo digital.

CENTROS DE SEGURIDAD EN INTERNET

El núcleo de la estrategia «Una Internet mejor para los niños» (BIK+) es una red de Centros de Seguridad en Internet, cofinanciados por la UE.

Tan solo en 2025, los Centros de Seguridad en Internet llegaron a más de 46,4 millones de europeos, organizaron 448 000 visitas y escuelas y sesiones de formación, y gestionaron más de 57 000 contactos a través de las líneas telefónicas de ayuda Insafe³¹⁰.

La red también es la promotora, junto con la Comisión Europea, del Día por una Internet más segura, la campaña mundial que se celebra cada año en febrero para sensibilizar sobre la seguridad en línea.

Los Centros de Seguridad en Internet ofrecen una serie de servicios que abordan tanto la prevención como el apoyo. Ofrecen sesiones de formación y material de uso fácil para las familias y las escuelas, con el fin de reforzar la alfabetización digital y promover un comportamiento responsable en línea.

Muchos Centros de Seguridad en Internet de toda Europa han sido designados como «alertadores fiables» en virtud del Reglamento de Servicios Digitales, lo que refuerza la protección de los menores en línea al permitir la denuncia prioritaria de contenidos ilícitos que afecten a niños y jóvenes. Los Centros desempeñan un papel crucial a la hora de informar a los coordinadores de servicios digitales sobre los riesgos que afectan a los niños y los jóvenes, contribuyendo así a la aplicación del Reglamento de Servicios Digitales³¹¹.

Los Centros también gestionan líneas telefónicas de ayuda, que prestan apoyo directo a los niños y las familias que se enfrentan a riesgos en línea, como el ciberacoso, y líneas directas que permiten denunciar de forma anónima presuntos materiales de abuso sexual de menores.

Los Centros de Seguridad en Internet llevan a cabo campañas de sensibilización a escala nacional y europea para promover la seguridad y el empoderamiento de los niños en línea. Esto incluye iniciativas específicas, como «DSA for YOUth», que explica el Reglamento de Servicios Digitales de la UE y sus directrices sobre la protección de menores de manera accesible para los jóvenes.

En términos más generales, las campañas de sensibilización contribuyen a informar a los niños, los cuidadores y los educadores sobre los riesgos en línea para los menores y las prácticas seguras. Esto incluye iniciativas que abordan la exposición a dispositivos digitales durante la primera infancia.

EDUCACIÓN Y ALFABETIZACIÓN DIGITALES

Los Estados miembros de la UE son responsables de la organización de los sistemas nacionales de educación y formación, de los planes de estudios y de la impartición de educación y formación. La UE apoya la colaboración y el intercambio de buenas prácticas entre los Estados miembros y proporciona apoyo financiero a iniciativas de educación y formación a través de programas de la UE, incluido Erasmus+.

En marzo de 2025, la Comisión Europea adoptó la Estrategia de la Unión de las Competencias. La Unión de las Competencias tiene por objeto reforzar la adquisición de competencias básicas y avanzadas, incluidas las digitales, en toda la UE mediante la promoción del aprendizaje permanente. Una piedra angular de la estrategia es el Plan de Acción para las Competencias Básicas, cuyo objetivo es abordar las deficiencias en la adquisición de competencias básicas, incluidas las competencias digitales y ciudadanas^b.

Las conclusiones del Estudio Internacional sobre Competencia Digital (ICILS) de 2023 indican que el 42,5 % de los jóvenes de entre 13 y 14 años carecen de competencias básicas en alfabetización informática y en materia de información³¹². El contexto socioeconómico es un factor predictivo importante de la alfabetización informática y en materia de información. La tasa de bajo rendimiento de los alumnos con al menos un progenitor que ha completado estudios universitarios es 16 puntos porcentuales inferior a la de los niños cuyos progenitores tienen un nivel de cualificación más bajo (32,4 y 48,6 %, respectivamente)³¹³.

Además, los últimos datos del Estudio Internacional sobre la Enseñanza y el Aprendizaje (TALIS) de la OCDE muestran que solo el 45,9 % de los profesores de los Estados miembros de la UE se sienten prepa-

b. Las competencias ciudadanas se refieren a la capacidad de actuar de manera responsable y participar plenamente en la vida cívica, así como a competencias como el pensamiento crítico (pertinente para interactuar de manera constructiva con la inteligencia artificial) y la alfabetización mediática.

rados para utilizar recursos y herramientas digitales en la enseñanza³¹⁴. Estos datos ponen de relieve la necesidad no solo de reforzar las competencias y la alfabetización digitales de los alumnos, sino también las de los profesores y educadores mediante la mejora de la formación inicial y continua del profesorado para ayudar a proteger y empoderar a los niños y adolescentes en línea.

A escala de la UE, la iniciativa del Espacio Europeo de Educación promueve el desarrollo de un «enfoque escolar integral y sistémico» para abordar la salud mental y el bienestar en las escuelas y crear entornos de aprendizaje positivos. Los Estados miembros de la UE han reconocido la importancia de apoyar a los progenitores, las escuelas y los profesores en la promoción de la salud mental y el bienestar de los niños³¹⁵.

Las consultas con progenitores y cuidadores muestran que los progenitores a menudo se sienten abrumados y que están «constantemente tratando de ponerse al día» con los últimos avances tecnológicos en el entorno de los medios sociales+. Al mismo tiempo, el conocimiento sobre cómo apoyar a los niños cuando se encuentran con contenidos nocivos o ilícitos suele ser limitado³¹⁶.

Los Estados miembros también han destacado la necesidad de que los proveedores de medios sociales y otros servicios digitales se abstengan de utilizar prácticas de diseño intencionadamente adictivas dirigidas a los niños y promuevan un diseño de los medios sociales y otros servicios digitales adecuado a la edad³¹⁷.

PLAN DE ACCIÓN DE EDUCACIÓN DIGITAL

La educación y la alfabetización digitales son fundamentales para dotar a los niños y adolescentes de las competencias que necesitan para navegar con seguridad por el mundo en línea. Sin embargo, las competencias y la alfabetización digitales de los niños y adolescentes van a la zaga del ritmo de los cambios tecnológicos en el entorno de los medios sociales y otros servicios digitales, contrariamente a la idea de que los menores de hoy son «nativos digitales».

Es fundamental integrar las competencias y la alfabetización digitales en los sistemas educativos nacionales. Según una encuesta del Eurobarómetro de 2025, el 92 % de los europeos está de acuerdo en que las competencias digitales deben enseñarse a todos en todos los niveles educativos y en que las escuelas deben enseñar a los alumnos cómo gestionar el impacto de las tecnologías digitales (incluidas los medios sociales) en su salud mental y física³¹⁸.

Para ayudar a los Estados miembros de la UE a impartir una educación digital de alta calidad, inclusiva y accesible, la Comisión Europea está aplicando el Plan de Acción de Educación Digital (2021-2027). El

«Posicionar la formación del profesorado como un pilar no legislativo para la seguridad en línea de los niños [...] Incorporar la educación digital en todos los programas de formación docente de manera integral y capacitar a los profesores para que colaboren eficazmente con los progenitores.»

— LOUISE HEERAN FLYNN,
PROFESORA ADJUNTA DE FORMACIÓN
DOCENTE, TRINITY COLLEGE DUBLIN

Plan permite a los Estados miembros de la UE adaptar sus sistemas educativos a los rápidos cambios tecnológicos y a la creciente importancia de las competencias digitales.

Las dos principales prioridades estratégicas del Plan de Acción de Educación Digital son la creación de un ecosistema europeo sólido de educación digital y la mejora de las habilidades y competencias digitales. Concretamente, el Plan apoya la mejora de las infraestructuras y los entornos de aprendizaje digital, la conectividad a internet y los equipos digitales en las escuelas, el suministro de contenidos y plataformas de aprendizaje digital de alta calidad y la formación del profesorado en el uso de herramientas y pedagogías digitales.

Como parte del Plan de Acción de Educación Digital, en marzo de 2026 la Comisión publicó cuatro conjuntos de directrices³¹⁹ destinadas a apoyar a los profesores y educadores en cuestiones como la lucha contra la desinformación y la promoción de la alfabetización digital, el uso ético de la IA y los datos en la educación, los contenidos educativos digitales de alta calidad y la enseñanza de la informática.

Las directrices para profesores y educadores sobre la lucha contra la desinformación y la promoción de la alfabetización digital a través de la educación y la formación ofrecen recursos sobre el uso informado y seguro de los medios sociales, la IA generativa y la intervención preventiva frente a la desinformación («prebunking»)^c, y ofrecen planes didácticos para que los profesores aborden el ciberacoso, junto con temas como los estereotipos de género y las ultrafalsificaciones³²⁰.

En el marco del Plan de Acción de Educación Digital, el Centro Europeo de Educación Digital ofrece una comunidad en línea que reúne a educadores, responsables políticos, investigadores y otras partes interesadas. A través del Centro, comparten conocimientos y buenas prácticas y crean conjuntamente soluciones de educación digital. El Centro también ayuda a los profesores y educadores a establecer contactos y participar en actividades relacionadas con la educación digital, como el aprendizaje entre iguales.

Además, los programas Erasmus+ y el Cuerpo Europeo de Solidaridad, la Plataforma Europea de Educación Escolar y la comunidad eTwinning ofrecen apoyo adicional para empoderar a los menores y a los educadores en línea. Esto incluye oportunidades de aprendizaje no formal y participación, así como apoyo a espacios en los que las comunidades escolares puedan interactuar, crecer y desarrollar sus competencias.

A finales de 2026, la Comisión Europea pondrá en marcha un paquete de medidas sobre educación. El paquete contribuirá a preparar los ecosistemas educativos nacionales para el futuro abordando los retos estructurales, incluida la necesidad de una infraestructura educativa digital europea segura, soberana y fiable. El paquete ayudará a dotar a los niños y adolescentes de competencias esenciales para interactuar de manera constructiva con la IA y las tecnologías digitales, esforzándose por integrar el bienestar y la alfabetización digitales, así como la seguridad en línea, en los sistemas educativos nacionales.

c. El «prebunking» es una medida preventiva que tiene por objeto preparar al público para que sea capaz de reconocer y hacer frente a los riesgos relacionados con la información, incluida la información errónea y la desinformación.

CAMPAÑA «AI≠HUMAN – TALK TO A PERSON»

Las iniciativas de sensibilización a escala nacional, incluida la campaña «AI≠Human – Talk to a person», ilustran la importancia de ayudar a los niños y adolescentes a comprender la naturaleza y las limitaciones de las herramientas basadas en la IA, incluidos los chatbots, y a aprender a utilizarlas de forma crítica y responsable.

Estas iniciativas transmiten un mensaje claro a los niños y adolescentes: si bien la inteligencia artificial puede ser una herramienta útil cuando se utiliza con las salvaguardias adecuadas, no puede sustituir a las relaciones humanas.

La campaña se llevó a cabo en la primavera de 2026 y fue desarrollada por el Ministerio de Educación, Infancia y Juventud de Luxemburgo, en colaboración con el Centro de Seguridad en Internet «BEE SECURE», el Centro de Apoyo Psicosocial y Escolar (CePAS) y la asociación de estudiantes luxemburguesa (CNEL).

Llamó la atención sobre una serie de riesgos potenciales asociados al uso no crítico o excesivo de la IA. Entre ellos se incluyen la posibilidad de un mayor aislamiento social, el uso de la IA como sustituto de la interacción humana y una disminución del diálogo real y de la comunicación cara a cara.

Además, la campaña pone de relieve las preocupaciones relacionadas con la «descarga cognitiva», en referencia a situaciones en las que los usuarios dependen cada vez más de los sistemas de IA para estructurar sus pensamientos, generar respuestas o tomar decisiones. Esto puede reducir las oportunidades de reflexión independiente y de participación cognitiva activa. La campaña también subraya problemas relacionados con la protección de datos y la privacidad en relación con el uso de la IA.

MARCO DE ALFABETIZACIÓN EN IA

En junio de 2026, la OCDE y la Comisión Europea presentaron un marco de alfabetización en materia de IA para la educación primaria y secundaria³²¹. La iniciativa promueve enfoques comunes para el desarrollo de la alfabetización en materia de IA en los sistemas educativos nacionales.

El marco apoya a los profesores, los sistemas educativos y las escuelas a la hora de dotar a los niños de las competencias que necesitan para comprender la IA e interactuar con ella de manera crítica. Su objetivo es capacitar a los niños para que interactúen de forma segura con la IA, gestionen y orienten su desarrollo y evalúen de forma crítica las oportunidades y los riesgos que presentan estas herramientas.

PARTICIPACIÓN DE LOS NIÑOS

Los niños y adolescentes deben disponer de oportunidades significativas para participar en la vida democrática y tomar parte de forma sistemática en las decisiones que afectan a su vida cotidiana. Esto incluye el diseño y la aplicación de políticas que promuevan la protección y el empoderamiento de los menores en línea.

La participación significativa de los niños se basa en el respeto mutuo, la transparencia y el carácter voluntario de la participación. Toda participación en la que intervengan niños debe proporcionar in-

«Los esfuerzos para mejorar la seguridad infantil en línea deben centrarse en crear entornos digitales seguros y de apoyo, al tiempo que se preservan las oportunidades de los niños para aprender, jugar, participar, comunicarse y acceder a la información.»

— ALEXANDRA WEILENMANN,
PROFESORA DE DISEÑO DE INTERACCIÓN,
UNIVERSIDAD DE GOTEBURGO

formación clara y adecuada a su edad sobre los objetivos y el proceso relacionados con su participación y establecer las salvaguardias adecuadas. Debe informarse claramente a los menores sobre cómo se utilizarán sus aportaciones.

Garantizar que los menores sean reconocidos como partes interesadas en las decisiones que configuran sus vidas es fundamental para defender sus derechos, tanto en línea como fuera de línea. El primer pilar de la Estrategia de la UE sobre los Derechos del Niño reconoce la importancia de la participación de los niños, promovida, por ejemplo, a través de la Plataforma de Participación Infantil de la UE.

Las acciones de participación juvenil, como el «control joven», los diálogos sobre políticas de juventud, el Comité Asesor Juvenil de la presidenta y el Diálogo de la UE con la Juventud, también desempeñan un papel importante en la mejora de la participación de los jóvenes en la elaboración de políticas a escala de la UE.

Al implicar activamente a los niños y adolescentes en los debates sobre la seguridad en línea, los res-

ponsables políticos no solo cumplen sus obligaciones jurídicas y éticas, sino que también aprovechan las perspectivas únicas de los menores a la hora de proteger y defender sus derechos en línea. Deben adoptarse medidas para garantizar la participación de los niños y adolescentes de diversos orígenes y zonas geográficas, a fin de garantizar la inclusividad y la eficacia de las medidas diseñadas para proteger y empoderar a los menores en línea.

Además, es fundamental que se empodere a los niños y adolescentes para que participen en la creación de un espacio seguro en el ámbito de los medios sociales y otros servicios digitales. Los proveedores de medios sociales y otros servicios digitales deben tratar las quejas de niños y adolescentes como una prioridad en los procedimientos de moderación de contenidos.

La Recomendación de la Comisión Europea sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia pide a los Estados miembros de la UE que garanticen la participación de los niños, un marco jurídico y político coherente para la protección de la infancia, mecanismos de denuncia y notificación seguros, confidenciales y adaptados a los niños, así como servicios y cuidados de calidad familiares y comunitarios³²².

PLATAFORMA DE PARTICIPACIÓN INFANTIL DE LA UE

Los menores tienen derecho a expresar libremente sus opiniones y a que estas se tengan en cuenta en los asuntos que les conciernen³²³. Para poner en práctica estos derechos, la Comisión Europea creó la Plataforma de Participación Infantil de la UE.

La Plataforma ofrece un espacio específico en el que los menores de 18 años pueden colaborar directamente con los responsables políticos y los responsables de la toma de decisiones. La Plataforma ofrece un espacio seguro para que los niños y adolescentes compartan sus puntos de vista y debatan temas que les afectan. La Plataforma organiza actividades, como reuniones, talleres, cursos de formación y encuestas en línea y presenciales, para recabar las opiniones de los niños.

A través de la Plataforma de Participación Infantil de la UE, la Comisión Europea ha consultado a miles de niños, en particular sobre cuestiones como el ciberacoso, la seguridad en línea, el bienestar digital y la próxima Ley de Equidad Digital. Este proceso ha dado lugar a la creación de un «Llamamiento a la acción dirigido a los responsables de la toma de decisiones de la UE»³²⁴ que aborda las cuestiones que más importan a los niños.

En el marco de estas consultas, los niños han destacado su deseo de participar activamente en la elaboración de las normas que afectan a sus actividades en línea. Muchos también han dejado claro que son los adultos, y no los niños, los responsables de cómo se han diseñado y funcionan hoy en día el mundo en línea y los medios sociales+, y que no se debe «castigar» a los niños por sus deficiencias.

El mensaje de los niños es claro: quieren que el mundo en línea sea más seguro, justo y fácil de entender, con normas más estrictas en los casos en que los servicios en línea puedan ser injustos, perjudiciales o adictivos. También han pedido alternativas a los medios sociales+, como actividades extraescolares y deportivas, y que los responsables de la toma de decisiones aborden los problemas de bienestar y salud mental relacionados con el uso de los medios sociales por parte de los niños.

RECOMENDACIONES DE LOS NIÑOS

Del 16 al 18 de abril de 2026, veinte niños y jóvenes de diferentes Estados miembros de la UE se reunieron en Berlín con motivo de la visita de estudio de la Plataforma de Participación Infantil de la UE sobre bienestar y salud mental.

A lo largo de dos días, compartieron, aprendieron y formularon recomendaciones sobre cómo los niños pueden sentirse seguros, apoyados, respetados y escuchados en relación con los problemas de salud mental, y cómo los adultos, las escuelas, las familias y los servicios pueden apoyar mejor el bienestar de los niños.

Como parte de la visita de estudio, los niños formularon varias recomendaciones sobre lo que necesitan para reforzar su bienestar:

- // Debemos tener libertad para permanecer en una conversación o abandonarla, disponer de un espacio seguro para expresarnos y saber a quién acudir;
- // Necesitamos sistemas de apoyo estables y fiables, estructuras que nos permitan ser escuchados y una comunidad en la que podamos confiar;
- // Debemos tener acceso a «vías de desahogo emocional»: ejercicio y deporte, aficiones, escribir un diario, relajación, espacios seguros para jugar y estar activos;

- // Las escuelas deben normalizar las conversaciones sobre salud mental e introducir jornadas periódicas para abordar el bienestar mental. Deben crearse entornos seguros en los que nos sintamos cómodos debatiendo nuestra salud mental y los profesores deben recibir formación para prestar apoyo en materia de salud mental, al igual que reciben formación en primeros auxilios. Cada escuela debe contar con un psicólogo o un orientador formado que sea realmente accesible y en quien los alumnos confíen;
- // Necesitamos una comunicación clara, abierta y eficaz con los adultos;
- // Necesitamos indicaciones claras para identificar a qué adultos podemos acudir en busca de ayuda en diferentes contextos y para diferentes problemas;
- // Los temas relacionados con la salud deben tratarse de forma adecuada en las escuelas, para que no tengamos que recurrir a los espacios en línea para colmar las lagunas^d.

Asesoramiento entre iguales

El asesoramiento entre iguales puede desempeñar un papel importante a la hora de promover el bienestar, tanto en línea como fuera de línea, entre los niños y adolescentes, al crear un entorno de apoyo en el que puedan hablar de sus dificultades con compañeros que han recibido formación. Dado que a los niños a menudo les resulta más fácil confiar en alguien cercano a su propia edad, el asesoramiento entre iguales puede fomentar la búsqueda temprana de ayuda y contribuir a evitar que los problemas se agraven, además de garantizar que exista un espacio seguro fuera de línea en el que puedan relacionarse y establecer vínculos significativos basados en experiencias compartidas.

«La verdadera seguridad en línea va más allá de la regulación. Requiere alfabetización digital, apoyo accesible e inversión en espacios fuera de línea.»

— MARTINA TÓTHOVÁ,
COMITÉ ASESOR JUVENIL DE LA
PRESIDENTA, CONSEJO DE LA JUVENTUD
DE ESLOVAQUIA

En el contexto de la seguridad infantil en línea, los compañeros asesores pueden ayudar a sensibilizar sobre los riesgos, como el ciberacoso, el uso saludable de pantallas y los medios sociales+, la información errónea y la desinformación, la inteligencia artificial y la importancia de proteger los datos personales. Los compañeros asesores pueden fomentar comportamientos digitales positivos, como la comunicación respetuosa, la empatía, el pensamiento crítico y la participación responsable en línea.

Dado que el apoyo procede de compañeros de una edad similar que comparten experiencias parecidas, el asesoramiento entre iguales suele percibirse como más cercano y creíble, y menos formal o intimidatorio para los niños y adolescentes a la hora de interactuar. Puede fomentar un

^d. En Bulgaria, por ejemplo, los niños informaron de que recibían información sobre temas de salud principalmente a través de herramientas de IA.

sentido de pertenencia, inclusión y apoyo mutuo en las escuelas o comunidades, empoderando a los menores para que desempeñen un papel activo a la hora de ayudarse mutuamente para tener experiencias seguras en línea.

EJEMPLOS DE BUENAS PRÁCTICAS EN EL ASESORAMIENTO ENTRE IGUALES

El Centro de Referencia para el Apoyo Psicosocial de la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (FICR) desarrolló el conjunto de herramientas **«Primeros auxilios psicológicos para jóvenes»**, con el fin de ayudar a los jóvenes a apoyar a sus compañeros en momentos difíciles³²⁵.

Este conjunto de herramientas empodera a los jóvenes al dotarlos de las competencias y los conocimientos necesarios para ayudar a sus compañeros, al tiempo que sensibiliza sobre la importancia del autocuidado³²⁶. El objetivo general del conjunto de herramientas es reforzar la resiliencia de los jóvenes cuando ante la adversidad y las situaciones de crisis, y dotarlos de conocimientos y competencias en materia de primeros auxilios psicológicos³²⁷. Incluye un manual que presenta el concepto de «primeros auxilios psicológicos» y ofrece ejemplos prácticos de cómo los jóvenes pueden aplicarlo para ayudar a sus compañeros³²⁸.

El conjunto de herramientas también ofrece un paquete de formación para escuelas, clubes juveniles y deportivos y organizaciones de escultistas. Los participantes aprenden cuáles son los retos que afectan a las personas de su edad, las situaciones de crisis y las reacciones ante ellas, para aplicar los principios básicos de los primeros auxilios psicológicos y las prácticas de autocuidado³²⁹. Los participantes también aprenden a reconocer cuándo alguien puede necesitar una ayuda que va más allá lo que ellos pueden proporcionar³³⁰.

Otro ejemplo de buenas prácticas es la iniciativa portuguesa **«Líderes Digitais»** (Líderes Digitales), desarrollada por el Centro de Sensibilización SeguraNet³³¹. A través de un enfoque entre iguales, la iniciativa capacita a los alumnos para actuar como embajadores digitales en sus escuelas.

Los alumnos participantes reciben formación sobre temas como la ciudadanía digital, la seguridad en línea, el ciberacoso, la privacidad y la protección de datos, la desinformación, la alfabetización mediática y el uso responsable de las tecnologías emergentes, incluida la inteligencia artificial. A continuación, comparten estos conocimientos con sus compañeros a través de actividades de sensibilización, talleres, debates en el aula y apoyo informal, contribuyendo así a una cultura digital más segura y positiva dentro de la comunidad escolar.

Las iniciativas dirigidas por compañeros, como «Líderes Digitais», demuestran cómo los niños pueden desempeñar un papel activo en la promoción del bienestar en línea y la resiliencia digital. Al fomentar el diálogo entre iguales, estas iniciativas fomentan comportamientos digitales positivos, como una comunicación respetuosa en línea, el pensamiento crítico, la empatía y la participación responsable en entornos digitales, al tiempo que refuerzan el sentido de pertenencia y el apoyo mutuo de los niños.

Sin embargo, el éxito a largo plazo y la escalabilidad de las iniciativas de asesoramiento entre iguales dependen de una financiación sostenida y del apoyo institucional para garantizar la continuidad y permitir

que más escuelas y niños se beneficien de ellas. Por lo tanto, es imperativo reconocer su valor e invertir en su desarrollo continuo, dada su importante contribución a la seguridad y el bienestar de los niños en línea.

Recomendaciones

RECOMENDACIÓN N.º 1

Ampliar las oportunidades seguras para que los niños participen activamente en la configuración del entorno de los medios sociales+

Los niños y adolescentes deben tener oportunidades significativas para configurar activamente la legislación, las políticas y las iniciativas educativas que promuevan la seguridad y el empoderamiento de los niños en línea. Debe ampliarse el uso de las herramientas de participación infantil y juvenil para fundamentar este trabajo. Más concretamente, debe incluirse a los niños en el diseño conjunto de las políticas de seguridad, los programas de formación, las evaluaciones y las directrices. Las medidas deben ser objeto de un seguimiento y una evaluación continuos para valorar su impacto en la seguridad y los derechos de los niños.

Los procesos de participación deben garantizar que los niños reciban información clara, comprendan cómo se utilizarán sus contribuciones y reciban comentarios sobre los resultados. Deben realizarse esfuerzos especiales para incluir a los niños de grupos desfavorecidos, marginados y vulnerables. Todas las actividades de participación que impliquen a niños deben ir acompañadas de medidas de salvaguardia adecuadas.

RECOMENDACIÓN N.º 2

Reforzar los mecanismos de denuncia y notificación, así como los derechos de los consumidores para niños y adolescentes

Los proveedores de medios sociales y otros servicios digitales deben dar prioridad a los informes y quejas de niños y adolescentes en los procedimientos de moderación de contenidos. Deben reforzarse las obligaciones de los proveedores en virtud de los marcos existentes para financiar adecuadamente las líneas telefónicas de ayuda y los mecanismos de reclamación. Estos mecanismos deben ser adecuados para la edad, fáciles de usar, accesibles, respetuosos de la privacidad y eficaces.

RECOMENDACIÓN N.º 3

Financiar y promover la creación y el uso de redes sociales y otros servicios digitales basados en valores de la UE en los que los menores puedan interactuar de forma segura entre sí

Apoyar, mediante inversión pública, la creación y la integración de medios sociales y otros servicios digitales basados en valores de la UE, concebidos para garantizar su seguridad y adecuados a la edad. Estos servicios deben garantizar la disponibilidad de información fiable que permita a los niños y adolescentes

(pero también a los adultos) mantener interacciones seguras en línea sin verse expuestos a características nocivas.

RECOMENDACIÓN N.º 4

Integrar acciones de educación y alfabetización digitales para menores, padres y cuidadores, profesores y educadores

La educación y la alfabetización digitales deben integrarse en todos los niveles educativos como una competencia básica clave para los menores, los padres y los profesores. El bienestar digital debe integrarse en la educación digital para todos.

La educación debe permitir a los niños y adolescentes evaluar de forma crítica la información y las fuentes en línea y reconocer las técnicas de manipulación, como la desinformación, las falsedades profundas y la publicidad personalizada. También debe lograr que los menores, los padres y los profesores comprendan cómo se crean y comparten los contenidos digitales y cómo los algoritmos configuran lo que los usuarios ven y experimentan en el mundo de los medios sociales y otros servicios digitales.

La educación estructurada en materia de seguridad en línea debe desarrollar competencias prácticas para proteger los datos personales, gestionar los ajustes de privacidad, mantener identidades digitales seguras e identificar los riesgos en los medios sociales y otros servicios digitales, los mensajes y los entornos de juego en particular. Estas capacidades deben desarrollarse progresivamente, empezando por los hábitos básicos de seguridad y avanzando hacia una comprensión más compleja de las huellas digitales, el consentimiento y los riesgos de las plataformas. El uso saludable de pantallas debe abordarse mediante orientaciones sobre el equilibrio, la gestión de la atención y el reconocimiento de patrones de uso excesivos o nocivos.

Los Centros de Seguridad en Internet deben seguir desempeñando un papel clave a la hora de ofrecer formación, actividades de sensibilización, recursos y apoyo a los niños, los progenitores, los cuidadores y los profesores. Debe financiarse el desarrollo de cursos en línea de fácil acceso para progenitores, profesores y jóvenes usuarios.

Además de la seguridad, la educación debe hacer hincapié en las oportunidades y el empoderamiento: cómo pueden utilizar los alumnos las herramientas digitales para el aprendizaje, la creatividad, la colaboración y la participación ciudadana.

RECOMENDACIÓN N.º 5

Crear más oportunidades e infraestructuras adecuadas para apoyar las actividades fuera de línea

Los Estados miembros y las autoridades locales deben mantener y ampliar el acceso a deportes, artes, clubes juveniles, bibliotecas y espacios comunitarios asequibles para fomentar una participación saludable en el mundo real y crear alternativas atractivas al uso excesivo de pantallas entre los menores. Esto debe incluir la inversión en entornos seguros, inclusivos y adaptados a la edad en los que los menores puedan conectar, aprender, jugar y establecer relaciones positivas dentro de sus comunidades.

RECOMENDACIÓN N.º 6**Promover la creación conjunta de directrices para los padres**

Junto con las asociaciones de progenitores, la UE y los Estados miembros deben promover el desarrollo de directrices para progenitores. Las directrices podrían proporcionar asesoramiento claro y accesible para capacitar a los padres y cuidadores a la hora de apoyar el uso seguro, responsable y positivo de los menores con los entornos de los medios sociales y otros servicios digitales. Las directrices deben proporcionar asesoramiento práctico sobre ámbitos clave, como la seguridad y la privacidad en línea, el bienestar digital, el uso ético y responsable y el acceso al apoyo.

RECOMENDACIÓN N.º 7**Garantizar que los padres y los cuidadores cuenten con el apoyo continuo de herramientas de control y supervisión de última generación y actualizadas**

Los esfuerzos por empoderar a los menores deben complementarse con un apoyo continuo a los progenitores y cuidadores, no solo en lo que respecta a las competencias y la alfabetización digitales, sino también con herramientas que permitan a los cuidadores orientar el uso que los menores hacen de los medios sociales y otros servicios digitales, sin restringir de manera desproporcionada los derechos de los niños. Esto incluye poner a su disposición y dar a conocer herramientas prácticas de supervisión parental, complementadas con información fiable sobre los riesgos, las prácticas seguras y la manera de interactuar con los niños. La sensibilización con los progenitores debe llevarse a cabo de forma presencial (por ejemplo, en reuniones con los profesores en la escuela, durante las visitas al pediatra, el embarazo o el permiso parental).

Las herramientas de supervisión parental deben ser eficaces, fáciles de utilizar, interoperables y adecuadas a la edad, en consonancia con la evolución de las capacidades de los menores, y estar diseñadas para fomentar la comunicación, el aprendizaje y el empoderamiento, en lugar del control. Esto es fundamental para promover el camino gradual de los menores hacia el uso autónomo de los medios sociales+. Estas herramientas deben garantizar que los cambios solo puedan realizarse con el mismo grado de autorización necesario para su activación, aplicarse independientemente del dispositivo o del sistema operativo, e incluir salvaguardias que informen a los menores sobre un posible uso indebido por parte de los progenitores (por ejemplo, una notificación clara a los menores cuando se activen las herramientas de supervisión).

RECOMENDACIÓN N.º 8**Garantizar una financiación pública suficiente y normas comunes para las organizaciones de la sociedad civil y el asesoramiento entre iguales**

La UE y los Estados miembros deben velar por que los Centros de Seguridad en internet y organizaciones comparables de la sociedad civil sigan recibiendo recursos financieros suficientes y su trabajo se base en normas comunes elaboradas por expertos. Esto es vital para mantener y seguir desarrollando sus actividades, incluidos los servicios de sensibilización, formación y apoyo.

La financiación pública es crucial para garantizar la independencia y la cohesión. La financiación también debe apoyar un mayor desarrollo del asesoramiento entre iguales, las líneas de ayuda, las líneas directas, los recursos educativos, las campañas de sensibilización y las actividades de desarrollo de capacidades. Deben destinarse inversiones adicionales para aumentar la visibilidad, la accesibilidad y el alcance de estos instrumentos, también entre los menores vulnerables, y para apoyar iniciativas que promuevan entornos más seguros en los medios sociales y otros servicios digitales.

RECOMENDACIÓN N.º 9

Permitir que el sistema sanitario diagnostique y trate las adicciones y otros trastornos de salud mental relacionados con el uso de las redes sociales y otros servicios digitales

Los sistemas sanitarios deben aplicar los criterios diagnósticos de la CIE-11 para las adicciones conductuales, incluido el trastorno del juego y el uso compulsivo de los medios sociales+. El tratamiento de estos trastornos basado en pruebas debe ser accesible dentro del sistema sanitario. Los profesionales médicos y los psicoterapeutas deben ser conscientes de las posibles consecuencias de los daños causados por la «negligencia digital» y la exposición involuntaria a contenidos inadecuados para la edad, el ciberacoso, la captación sexual en línea, la sextorsión y otros daños.

Los sistemas sanitarios deben ofrecer tratamientos basados en pruebas para el TEPT y otras consecuencias psicopatológicas. Además, los sistemas podrían integrar la evaluación de riesgos digitales en el cribado pediátrico y los enfoques de prevención selectiva para los menores vulnerables. Las medidas de prevención y los retos conductuales, como el «ayuno digital» o la «desintoxicación digital», podrían fomentar las experiencias fuera de línea y un cambio de cultura en relación con el uso de internet por parte de los menores.

RECOMENDACIÓN N.º 10

Apoyar la formación del profesorado para incluir la alfabetización digital y mediática e implicar a los padres

La UE y los Estados miembros deben garantizar que la formación inicial y continua del profesorado integre de forma sistemática las competencias y la alfabetización digitales, incluida la alfabetización en materia de IA, y el bienestar digital. Los profesores deben estar preparados para desarrollar la alfabetización crítica y mediática de los niños y adolescentes, junto con competencias digitales para un uso seguro de los medios sociales+.

Se debe sensibilizar a los profesores sobre el riesgo de la «sobredigitalización» en las escuelas. Cuando proceda, deben utilizarse nuevas herramientas digitales, como la IA, con fines pedagógicos específicos. La formación docente también debe incluir una estrecha colaboración con los progenitores para apoyar mejor el uso saludable y equilibrado de pantallas por parte de los menores, comprender cómo interactúan los niños y adolescentes con los medios sociales y otros servicios digitales, y desarrollar estrategias adecuadas a la edad para debatir los riesgos y experiencias en línea, tanto en el aula como en casa.

RECOMENDACIÓN N.º 11**Promover la alfabetización en materia de IA como parte integrante de la educación digital**

La alfabetización en materia de IA debe incorporarse a la educación digital en las escuelas y otras instituciones de educación y formación. Los menores deben comprender las oportunidades, las limitaciones y los riesgos asociados a las tecnologías de IA (por ejemplo, los chatbots o asistentes de IA, los sistemas de recomendación y la IA generativa), incluida la posibilidad de que haya información inexacta, manipulación y contenidos sintéticos.

La promoción de la alfabetización podría inspirarse en el marco de alfabetización en materia de IA para la educación primaria y secundaria desarrollado por la Comisión Europea y la OCDE. Los menores no deben estar expuestos a asistentes de IA antropomórficos que sugieran relaciones similares a las humanas sin supervisión.

RECOMENDACIÓN N.º 12**Las escuelas deben ofrecer oportunidades estructuradas para mejorar la salud mental y el bienestar digital**

Las escuelas deben desempeñar un papel proactivo a la hora de mitigar los riesgos de los medios sociales+ y favorecer la salud mental y el bienestar de los niños y adolescentes. Deben organizar sesiones informativas y formativas dirigidas a los progenitores, así como a los menores y sus progenitores, a fin de informar sobre la seguridad en línea, la salud mental y el bienestar.

Las escuelas deben ampliar el acceso al asesoramiento escolar y a otro tipo de apoyo a la salud mental para cuestiones relacionadas con el uso de los medios sociales+ por parte de los menores. Deben existir espacios físicos y en línea seguros y libres de estigmas en los que los alumnos se sientan capaces de hablar de sus dificultades (por ejemplo, en materia de salud mental, bienestar, etc.) derivadas de sus experiencias en línea en entornos de redes sociales+. Las escuelas deben tener acceso a profesionales cualificados en el ámbito de la salud y la asistencia social, incluida la atención escalonada en materia de salud mental. Los profesionales de la salud mental deben recibir formación especializada en bienestar digital y daños en línea.

Las escuelas también deben establecer mecanismos de denuncia accesibles, confidenciales y adaptados a los niños para los menores que experimenten problemas en línea. Para reforzar aún más la protección, las escuelas deben disponer de vías de derivación a servicios externos de protección de la infancia, salud mental y apoyo especializado.

RECOMENDACIÓN N.º 13**Las respuestas educativas deben prestar especial atención a los grupos vulnerables**

Los menores que se enfrentan a desventajas socioeconómicas, necesidades educativas especiales, experiencias adversas en la infancia, discriminación o dificultades de salud mental pueden estar expuestos a riesgos elevados en los medios sociales+. Las medidas educativas y de apoyo deben ser inclusivas,

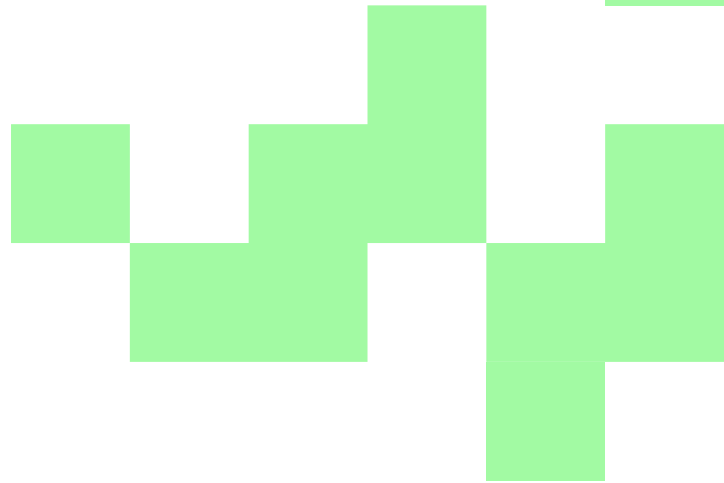
específicas cuando sea necesario y estar diseñadas para reducir las desigualdades tanto en los medios sociales como en la participación y el bienestar digitales.

En las escuelas, podrían ponerse en marcha intervenciones proactivas y específicas para abordar el impacto desproporcionado de los daños en línea sobre los menores vulnerables y marginados, con el fin de proteger y apoyar a los grupos vulnerables. Debe ampliarse el acceso equitativo a los dispositivos, la conectividad y las tecnologías asistenciales, también para los niños con discapacidad.

RECOMENDACIÓN N.º 14

Invertir en infraestructuras digitales educativas seguras, preventivas, sólidas y fiables

Las escuelas necesitan infraestructuras y herramientas digitales seguras, sólidas y fiables para reforzar las competencias digitales de los menores y garantizar la soberanía digital de Europa. Las escuelas europeas dependen en gran medida de aplicaciones de terceros países, y la adopción de soluciones desarrolladas en la UE se enfrenta a retos constantes. La UE debe priorizar y apoyar el desarrollo y la implantación de infraestructuras y herramientas digitales seguras e interoperables para la educación y reducir las dependencias estratégicas.



Agradecimientos

Nuestra tarea como copresidentes y consejeros especiales consistió en orientar y dirigir el proceso multi-nivel: la recopilación de conocimientos mediante la colaboración con expertos durante las reuniones del panel especial, la recopilación de pruebas de expertos y el mantenimiento de intercambios y contactos con numerosas partes interesadas.

El presente informe debe su existencia a un gran número de personas comprometidas con garantizar que los niños y adolescentes puedan navegar de forma segura por el mundo de los medios sociales+. Si bien la responsabilidad de las recomendaciones recae exclusivamente en nosotros, debemos mucho a las aportaciones de otros expertos de renombre, representantes de progenitores y jóvenes, y a la Comisión Europea.

En primer lugar, queremos expresar nuestro agradecimiento a la presidenta de la Comisión Europea, **Ursula von der Leyen**, por su constante interés y apoyo a nuestra labor. Su asistencia y participación en las reuniones del panel especial ponen de relieve su compromiso con la seguridad infantil en línea y fueron muy apreciadas por nosotros y por todos los participantes. Agradecemos a la presidenta su interés y dedicación constantes en relación con la seguridad infantil, lo que ha hecho posible llevar a cabo este trabajo y elaborar recomendaciones concretas para el bienestar de los niños y adolescentes de toda Europa. También queremos dar las gracias al jefe de gabinete de la presidenta, **Björn Seibert**, que acompañó todo el proceso desde el principio, y a **Patricia Reilly**, miembro del gabinete de la presidenta, por su apoyo constante.

Además, queremos dar las gracias a todos los participantes en las reuniones del panel especial. Agradecemos a todos aquellos que compartieron con nosotros una cantidad extraordinaria de conocimientos, experiencia y dedicación en beneficio de la juventud europea. Nos gustaría expresar nuestro especial agradecimiento a **Julie Inman Grant**, comisaria de eSafety de Australia, y a **Lucas Borges**, superintendente de regulación de la Agencia Brasileña de Protección de Datos, por proporcionarnos perspectivas y lecciones de sus respectivos países sobre la seguridad infantil en línea.

Hemos escuchado atentamente a todos, pero las conclusiones de este informe son responsabilidad nuestra.

AGRADECEMOS A LOS PARTICIPANTES DEL PANEL ESPECIAL*:

** lista no exhaustiva*

// **Ayata**, representante de 15 años de la Plataforma de Participación Infantil de la UE

// **Zuzanna**, representante de 17 años de la Plataforma de Participación Infantil de la UE

- // **Kimmo Alho**, psicólogo y profesor emérito, Universidad de Helsinki
- // **Mehdi Arfaoui**, sociólogo, Commission nationale de l'informatique
- // **Leanda Barrington-Leach**, directora ejecutiva, 5Rights Foundation
- // **Gabriele Battimelli**, embajador de Italia para «Una Internet mejor para los niños»
- // **Owen Bennett**, experto independiente en la regulación de las tecnologías digitales
- // **Elena Bozzola**, pediatra y consejera nacional de la Sociedad Italiana de Pediatría
- // **Matthias Brand**, profesor y jefe del Departamento de Psicología General, Universidad de Duisburgo
- // **Urs Buscke**, asesor jurídico principal, Oficina Europea de Uniones de Consumidores
- // **Ana Caballero**, presidenta, Grupo de expertos para la mejora de la protección de los menores en el ámbito digital (España)
- // **Alex Cooney**, directora general y cofundadora, CyberSafeKids
- // **Lies Craeynest**, fundadora, KidsUnplugged
- // **Jutta Croll**, presidenta, Stiftung Digitale Chancen
- // **María del Mar España Martí**, directora, Plataforma Control Z
- // **Sigge Eriksson**, presidente, Consejo Nacional de Organizaciones Suecas para la Infancia y la Juventud
- // **Marina Fernández**, presidenta, Adolescència Lliure de Mòbils
- // **Louise Flynn**, profesora adjunta, Trinity College Dublin
- // **Tobiáš Bruno Galia**, Consejo Checo de la Infancia y la Juventud
- // **Catalina Goanta**, profesora asociada de Derecho Privado y Tecnología, Universidad de Utrecht
- // **Konstantinos Karachalios**, asesor del director ejecutivo, IEEE y miembro del Consejo de Administración, Fundación 5Rights
- // **Maija Katkovska**, jefa, Centro de Seguridad en Internet de Letonia
- // **Rasmus Kjedadhl**, director, Børns Vilkår
- // **Petra Kogelnig**, secretaria general, Asociación Europea de Padres
- // **Pavel Kordik**, profesor asociado, Universidad Técnica Checa
- // **Marta Gonçalves**, embajadora de Portugal para «Una Internet mejor para los niños»
- // **Beckett LeClair**, jefe de Tecnología, Fundación 5Rights

- // **Sonia Livingstone**, profesora de Psicología Social, London School of Economics
- // **Aisling Maloney**, Consejo Nacional de la Juventud de Irlanda
- // **Giovanna Mascheroni**, profesora, Universidad Católica de Milán
- // **Helen Mason**, directora ejecutiva, Child Helpline International
- // **Elvira Mentzelioti**, presidenta, Consejo Nacional Helénico de la Juventud
- // **Eva Möhler**, presidenta y médica clínica de Psiquiatría Infantil y Adolescente, Universidad del Sarre
- // **Alberto Monge Roffarello**, profesor adjunto, Politecnico di Torino
- // **Théo Mouhoud**, psiquiatra infantil, Hopitaux de Paris
- // **Servane Mouton**, médica, neuróloga y neuropsicóloga
- // **Mie Oehlenschläger**, investigadora independiente y asesora sobre IA, ética y políticas públicas
- // **James O'Higgins Norman**, profesor de Educación y Sociedad, Dublin City University
- // **Maja Olszewska**, embajadora de Polonia para «Una Internet mejor para los niños»
- // **Brian O'Neill**, profesor emérito, Universidad Tecnológica de Dublín
- // **Kerstin Paschke**, médica especialista en Psiquiatría y Psicoterapia Infantil y Adolescente, Universitätsklinikum Hamburg-Eppendorf
- // **Leo Pekkala**, director adjunto, Instituto Audiovisual de Finlandia
- // **María Soledad Pera**, profesora asociada, TU Delft
- // **Tanja Petelin**, profesora asociada, Universidad de Poitiers
- // **Christoph Pieh**, jefe del Departamento de Medicina Psicosomática y Psicoterapia, Universidad de Formación Continua de Krems
- // **Jessica Piotrowski**, profesora, Universidad de Ámsterdam
- // **Declan Qualter**, supervisor de prácticas y candidato a doctorado, University College Dublin
- // **Kai Rannenberg**, profesor y jefe del Departamento de Negocios Móviles y Seguridad Multilateral, Universidad Johann Wolfgang Goethe de Fráncfort
- // **Anna Schwabegger**, presidenta del Consejo Nacional de la Juventud de Austria
- // **Judith Simon**, profesora de Ética de las Tecnologías de la Información, Universidad de Hamburgo
- // **Lore Sleenckx**, delegada europea de la juventud, Consejo Flamenco de la Juventud
- // **Petr Slovak**, profesor asociado de Interacción Hombre-Ordenador, King's College London

- // **Elisabeth Staksrud**, profesora, Departamento de Medios y Comunicación, Universidad de Oslo
- // **Sophie Stalla-Bourdillon**, jefa de investigación, Law, Science, Technology & Society Research Group, VUB
- // **Argyris Stringaris**, científico clínico y presidente, Psiquiatría Infantil y Adolescente, University College London
- // **Lisa Thorell**, profesora, Departamento de Neurociencia Clínica, Karolinska Institutet
- // **Hanne-Mari Schiøtz Thorud**, fisióloga y profesora, Universidad del Sureste de Noruega
- // **Piotr Toczyski**, profesor asociado, Universidad APS Maria Grzegorzewska
- // **Antonia Torrens**, presidenta, COFACE Families Europe
- // **Martina Tóthová**, delegada principal, Consejo de la Juventud de Eslovaquia
- // **Dimitris Tsalavos**, embajador de Chipre para «Una Internet mejor para los niños»
- // **Laura Vandenbosch**, profesora asociada y directora del Laboratorio de Psicología Mediática, KU Leuven
- // **Sørine Vesth Rasmussen**, asesora sobre derechos del niño y política tecnológica, Børns Vilkår
- // **Mieke Visser-Schuurman**, directora de Derechos del Niño y Desarrollo de Capacidades, Eurochild
- // **Rareș Voicu**, presidente, Foro Europeo de la Juventud
- // **Alexandra Weilenmann**, profesora del Departamento de Tecnologías de la Información Aplicadas, Universidad de Gotemburgo
- // **Niels Zagema**, representante de la juventud neerlandesa, Nationale Jeugdraad

Para nosotros, era fundamental garantizar no solo la representación de los jóvenes como participantes en las reuniones del panel especial, sino también implicarlos en la elaboración conjunta de este informe. Por ello, queremos dar las gracias a **Marta Gonçalves**, que no solo se unió al panel como embajadora de Portugal para «Una Internet mejor para los niños», sino que contribuyó a la elaboración de este informe.

Este informe no habría sido posible sin el apoyo de numerosos miembros del personal de la Comisión Europea.

En primer lugar, queremos agradecer a IDEA y a su director en funciones, **David Müller**, por acogernos y ofrecernos unas excelentes condiciones de trabajo.

Nuestro trabajo se benefició enormemente del apoyo de un equipo específico dentro de IDEA: queremos agradecer a **Undine Ruge** por la supervisión y el apoyo prestados durante el proceso. Debemos mucho a **Asen Dimitrov**, que, como coordinador principal de los copresidentes del panel especial sobre seguridad infantil en línea, fue nuestra extraordinaria persona de contacto, proporcionándonos asistencia, asesoramiento y apoyo tanto en el proceso como en el contenido, además de impulsar la realización

de nuestros planes, gestionar todas las reuniones e intercambios y coordinar el trabajo sobre el informe dentro de IDEA y, junto con los compañeros de la Secretaría General, también en el seno de la Comisión.

Este informe no habría visto la luz sin el apoyo adicional de IDEA: queremos dar las gracias a **Thomas Hopkins**, que fue un excelente editor de la versión inglesa del informe; a **Anna Magdalena Comploi**, que aportó sus conocimientos especializados y sus investigaciones y ayudó en todos los aspectos organizativos, así como a **Quinlan Rijks**, que participó en la elaboración de los elementos visuales. También queremos agradecer a **Alexander Hempfing** por su análisis y a **Yee-Sol Chang** y **Konrad Rose** por su participación.

Junto con IDEA, los compañeros de la Secretaría General han coordinado el trabajo realizado en el seno de la Comisión y han aportado información valiosa, tanto en lo que respecta al proceso como al contenido. Por lo tanto, damos las gracias al secretario general adjunto **Nils Behrndt** por su tiempo y dedicación, así como a **Nacira Boulehouat**, **Ioana-Maria Gligor**, **Alessandra Falcinelli**, **Tarik Draidj**, **Louis Dancourt** y **Armande Lorentz**.

En primer lugar, nos propusimos comprender mejor la legislación vigente y las herramientas existentes de que disponen la UE y los Estados miembros para proteger a los niños y adolescentes en línea, así como su aplicación hasta la fecha. Este contexto nos sirvió de base para debatir con expertos las lagunas actuales y el camino a seguir. Por ello, agradecemos el liderazgo de la DG CNECT y su director general, **Roberto Viola**, y su directora general adjunta, **Renate Nikolay**, y de la DG JUST y su directora general, **Ana Gallego Torres**, y su director general adjunto, **Hubert Gambs**.

Agradecemos a los expertos de la DG CNECT que aportaron valiosos conocimientos y perspectivas: **Prabhat Agarwal**, **Julia Van Best**, **Martin Harris Hess**, **Andrea Tognoni**, **Manon Baert**, **Emma O'Mahony** e **Irene Roche Laguna**.

Agradecemos a los expertos de la DG JUST que también aportaron valiosos conocimientos y perspectivas: **Maria-Myrto Kanellopoulou**, **Benedicte Van Ormelingen**, **Denisa Alexandroaiei**, **Caoimhe Sheridan**, **Marie-Cécile Rouillon** y **Marta Kuljon**.

Este informe se ha beneficiado de la investigación y las aportaciones de expertos de diferentes departamentos de la Comisión Europea (JRC, DG SANTE, DG EAC, DG HOME, DG RTD, DG GROW, SJ y otros): **Andrea Ceglia**, **Yves Punie**, **Marianne Takki**, **Martine Ingvorsen**, **Francesca Maltauro**, **Marta Touykova**, **Chiara Colella**, **Marta Markowska**, **Leonie Wahlmann**, **Katarzyna Janicka-Pawlowska**, **Veronica Travisani**, **Alessia Donna**, **Eva Gerhards**, **María del Pilar González Pantaleón**, **Amaryllis Verhoeven**, **Philipp Runge**, **Lorna Armati** y **Paul-John Loewenthal**.

Agradecemos a todos su experiencia y paciencia a la hora de responder a nuestras innumerables preguntas, así como su capacidad para sintetizar y hacer comprensibles cuestiones jurídicas y técnicas complejas.

También queremos dar las gracias a los expertos de la DG COMM y la SG, que nos prestaron un excelente apoyo en aspectos relacionados con la comunicación: **Chloe Lahousse Juarez**, **Anguel Konstantinov Beremliysky**, **Emma Kristina Kvennberg** y otros. Asimismo, a los diseñadores gráficos y expertos en traducción, que han demostrado una gran creatividad y paciencia: **Laurie Janssen**, **Camille Palandjian**, **Benedetta Benedetto** y otros.

Nuestro trabajo no habría sido posible sin el apoyo organizativo de numerosos compañeros de la Comisión para las reuniones del panel especial, los desplazamientos y otras reuniones con las partes interesadas:

Carmen Tresguerres, Rozaliya Petkova, Martina Gunda, Nuria Paredes, Alexandre Verin, Mariola De Las Heras Ojeda, Anne Catherine Louppe, Margarita Biacho Varela, Hafize Balci y Vaia Tsiampazi.

Como copresidentes, también nos hemos beneficiado del apoyo de nuestras instituciones de origen y de nuestros colaboradores más cercanos sobre el terreno:

Equipo del Prof. Dr. Fegert del Hospital Universitario de Ulm: **PD Dr. Franziska Köhler-Dauner, Prof. Dr. adjunta Ann-Christin Haag, Emily Sitarski, Lena Peter, Karen Schlaegel, Claudia Rau, Annette Claus y Ariane Saccarello.**

Equipo de la Dra. Maria Melchior del Instituto de Salud Pública de la Sorbona con la Universidad de la Sorbona y el Instituto Nacional de Salud e Investigación Médica de Francia (INSERM): **Fabienne El Khoury, Camille Davisse-Paturet, Hamid Massoumi, Bertrand Redonnet y Mays Kabakibi.**

Notas finales

01. Aries, P. (1962). *Centuries of childhood: A social history of family life*. Knopf Doubleday Publishing Group.
02. Berk, L.E. (1994). *Infants and Children Prenatal Through Early Childhood*.
03. Kessler, R. C., Magee, W. J. (1993). Childhood adversities and adult depression: basic patterns of association in a US national survey. *Psychological Medicine*, 23(3), 679–690.
04. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
05. Rideout, V. (2020). The Common Sense Census: Media Use by Kids Age Zero to Eight.
06. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
07. Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
08. Montag, C., Lachmann, B., Herrlich, M., Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International journal of environmental research and public health*, 16(14), 2612.
09. Steinberg, L. D. (2014). *Age of opportunity: Lessons from the new science of adolescence*. Houghton Mifflin Harcourt.
Casey, B. J., Getz, S., Galvan, A. (2008). The adolescent brain. *Developmental review*, 28(1), 62–77.
10. Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324.
Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). *Digital Media Use and Child Health and Development*. Deakin University. Journal contribution.
- Jing, X., et al. (2023). Effects of foreground screen media use on vocabulary development in young children: A meta-analysis. *Child Development*, 94(5), 1398–1415.
11. Johnston MV. Neurotransmitters and vulnerability of the developing brain. *Brain Dev.* 1995 Sep-Oct;17(5):301-6.
12. Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351–358.
Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
13. Boxer, P., Groves, C. L., Docherty, M. (2015). Video games do indeed influence children and adolescents' aggression, prosocial behavior, and academic performance: A clearer reading of Ferguson (2015). *Perspectives on psychological science*, 10(5), 671–673.
Coyne, S. M., Radesky, J., Collier, K. M., Gentile, D. A., Linder, J. R., Nathanson, A. I., Rogers, J. (2017). Parenting and digital media. *Pediatrics*, 140(Supplement 2), S112–S116.
14. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
15. Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
16. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93–117). Academic Press.
Mallawaarachchi S., Burley J., Mavilidi M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2024;178(10):1017–1026.
17. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during

- digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
- 18.** American Academy of Pediatrics (2024). Screen time guidelines. Center of Excellence on Social Media and Youth Mental Health.
- 19.** Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
- 20.** Li, C., Cheng, G., Sha, T., Cheng, W., Yan, Y. (2020). The relationships between screen use and health indicators among infants, toddlers, and preschoolers: A meta-analysis and systematic review. *International Journal of Environmental Research and Public Health*, 17(19), 7324. Ahmer, A., Raza, M., Azhar, M., Rahman, A., Das, J. K., Jafri, S. K. (2025). A systematic review and meta-analysis on the impact of screen-time on the social-emotional development of children under five years. *Journal of the College of Physicians and Surgeons Pakistan*, 35(3), 351-358.
- 21.** Bochicchio, V., Keith, K., Montero, I., Scandurra, C., Winsler, A. (2022). Digital media inhibit self-regulatory private speech use in preschool children: The “digital bubble effect”. *Cognitive development*, 62, 101180.
- 22.** Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631-650. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543.
- 23.** Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
- 24.** Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
- 25.** Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press. Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
- 26.** Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250. Mallawaarachchi S., Burley J., Mavilidi, M., et al (2024). Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes: A Systematic Review and Meta-analysis. *JAMA Pediatr*. 2024;178(10):1017-1026.
- 27.** Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent-child reading as support for children's language. *First language*, 33(5), 504-523. Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614.
- 28.** Kidron, B., Evans, A., Afia, J., Adler, J. R., Bowden-Jones, H., Hackett, L., Juj, A., Przybylski, A. K., Rudkin, A., Young Scot. (2018). Disrupted childhood: The cost of persuasive design. 5Rights Foundation. Stoilova, M., Bulger, M., Livingstone, S. (2024). Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use. *Journal of Children and Media*. Chao, M., Lei, J., He, R., Jiang, Y., Yang, H. (2023). TikTok use and psychosocial factors among adolescents: Comparisons of non-users, moderate users, and addictive users. *Psychiatry Research*, 325, 115247.
- 29.** Taylor, G., Sala, G., Kolak, J., Gerhardstein, P., Lingwood, J. (2024). Does adult-child co-use during digital media use improve children's learning aged 0–6 years? A systematic review with meta-analysis. *Educational Research Review*, 44, 100614. Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelus, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
- 30.** Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
- 31.** Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical*

- child and family psychology review, 24(3), 631-650. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
32. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
33. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543. 34.
34. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Jackson, D. B., Testa, A., Fox, B. (2021). Adverse childhood experiences and digital media use among US children. *American journal of preventive medicine*, 60(4), 462-470.
35. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601-17619. Zgambo, M., Anyango, E., Arabiat, D. H., Ngune, I., Mörelius, E., Zhang, M., Whitehead, L. C. (2025). Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR Pediatrics and Parenting*, 8(1), e70745.
36. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press. Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
37. Böttger, T., Zierer, K. (2024). To ban or not to ban? A rapid review on the impact of smartphone bans in schools on social well-being and academic performance. *Education Sciences*, 14(8), 906.
38. Boztas, S. (2025, July 4). Smartphone bans in Dutch schools have improved learning, study finds. The Guardian.
39. Wedekind, K. (2026, March 11). So abgelenkt sind Schüler, wenn es kein Handyverbot gibt. n-tv.
40. Korat, O., Shamir, A., Heibal, S. (2013). Expanding the boundaries of shared book reading: E-books and printed books in parent-child reading as support for children's language. *First language*, 33(5), 504-523.
41. Calvert, S. L. (2017). Parasocial relationships with media characters: Imaginary companions for young children's social and cognitive development. In *Cognitive development in digital contexts* (pp. 93-117). Academic Press. Marshall, S. J., Biddle, S. J., Gorely, T., Cameron, N., Murdey, I. (2004). Relationships between media use, body fatness and physical activity in children and youth: a meta-analysis. *International journal of obesity*, 28(10), 1238-1246.
42. Purba, A. K., Thomson, R. M., Henery, P. M., Pearce, A., Henderson, M., Katikireddi, S. V. (2023). Social media use and health risk behaviours in young people: systematic review and meta-analysis. *bmj*, 383.
43. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229-234. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
44. Schwartz, D., Zhang, M., Troop-Gordon, W., Taylor, L. M., Chung, J. (2025). Are social media use and popularity in the peer group linked during adolescence? A meta-analytic review. *Journal of Adolescence*, 97(3), 575-592.
45. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244-250. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
46. Children's Hospital of Philadelphia (2026). Age Limits Alone Won't Fix Smartphone Risks, Suggests Children's Hospital of Philadelphia Study. Accessed on 12 July 2026.
47. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513-543. Teague, S., Somoray, K., Shatte, A. Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
48. Nesi, J., Choukas-Bradley, S., Prinstein, M. J. (2018). Transformation of adolescent peer relations in the social media context: Part 1 – A theoretical framework and application to dyadic peer relationships. *Clinical child and family psychology review*, 21(3), 267-294. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67-S70.
49. Werling, A. M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with attention-deficit/hyperactivity disorder compared to controls: A meta-analysis. *Journal of Behavioral Addictions*, 11(2), 305-325.

50. Nesi, J., Telzer, E. H., Prinstein, M. J. (2020). Adolescent Development in the Digital Media Context. *Psychological Inquiry*, 31(3), 229–234.
Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
51. Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
52. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
53. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
54. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25(1), 79–93.
Liu, M., Kamper-DeMarco, K. E., Zhang, J., Xiao, J., Dong, D., Xue, P. (2022). Time spent on social media and risk of depression in adolescents: A dose-response metaanalysis. *International Journal of Environmental Research and Public Health*, 19.
55. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
56. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-analysis. *Education and Information Technologies*, 29(13), 17601–17619.
57. Yang, C. C., Holden, S. M., Ariati, J. (2021). Social media and psychological well-being among youth: The multidimensional model of social media use. *Clinical child and family psychology review*, 24(3), 631–650.
58. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
59. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
Orben, A., Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182.
60. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
61. Uhls, Y. T., Ellison, N. B., Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics*, 140 (Supplement 2), S67–S70.
62. Orben, A., Meier, A., Dalgleish, T., Blakemore, S. J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, 3(6), 407–423.
63. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
64. Vasconcellos, R. P., Sanders, T., Lonsdale, C., Parker, P., Conigrave, J., Tang, S., Noetel, M. (2025). Electronic screen use and children's socioemotional problems: A systematic review and meta-analysis of longitudinal studies. *Psychological Bulletin*, 151(5), 513–543.
65. Madigan, S., Browne, D., Racine, N., Mori, C., Tough, S. (2019). Association between screen time and children's performance on a developmental screening test. *JAMA pediatrics*, 173(3), 244–250.
Teague, S., Somoray, K., Shatte, A., Miller, D., Moss, K., Crawford, A. et al. (2026). Digital Media Use and Child Health and Development. Deakin University. Journal contribution.
66. Qian, H., Wang, C., Li, H. (2024). Parental risk factors and moderators of prolonged digital use in preschoolers: a meta-. *Education and Information Technologies*, 29(13), 17601–17619.
67. Pagano, M., Bacaro, V., Crocetti, E. (2023). "Using digital media or sleeping... that is the question". A meta-analysis on digital media use and unhealthy sleep in adolescence. *Computers in Human Behavior*, 146, 107813.
68. Odgers, C. L., Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
69. Sala, A., Porcaro, L., Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, volume 14.
70. Staksrud, E., Livingstone, S. (2009). Children and online risk. *Information, Communication and Society*, 12 (3).

71. Fegert, J.M. (2026). European child and adolescent psychiatry in a digital world. *European Child and Adolescent Psychiatry*, 35, 309–315.
72. WeProtect (2021). Estimates of childhood exposure to online sexual harms and their risk factors, p.5.
73. European Commission (2026). Action Plan against Cyberbullying.
74. Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *Journal of the American Medical Association Southeast Asia. Supplement. Pediatrics*, 169, 770–777.
Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
75. European Commission (2021). Study to support the preparation of the European Commission's initiative to extend the list of EU crimes in Article 83 of the Treaty on the Functioning of the EU to hate speech and hate crime. Final report.
76. European Institute for Gender Equality (EIGE). 2026. Growing up online: how violence follows girls across platforms. Accessed on 29 June 2026.
77. Abendroth Dias, K., Arias Cabarcos, P., Bacco, F.M., Bassani, E., Bertoletti, A., et al. (2025). Generative AI Outlook Report – Exploring the Intersection of Technology, Society and Policy. Navajas Cawood, E., Vespe, M., Kotsev, A., van Bavel, R. (editors). Publications Office of the European Union, Luxembourg, JRC142598.
78. Ofcom. (2024). A deep dive into deepfakes that demean, defraud and disinform. Accessed on 29 June 2026.
79. Rousay, V. (2023). Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms. Master's thesis, Harvard University Division of Continuing Education.
80. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
81. McCrae, N., Gettings, S., Pursell, E. (2017). Social media and depressive symptoms in childhood and adolescence: A systematic review. *Adolescent Research Review*, Vol. 2, pp. 315–330.
82. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
83. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
84. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
85. Twenge J.M., Martin G.N. (2020). Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets. *Journal of Adolescence*, 79, 91-102.
86. Svensson, R., Johnson, B. Olsson, A. (2022). Does gender matter? The association between different digital media activities and adolescent well-being. *MC Public Health*, 10 (22), 273.
87. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
88. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
89. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behaviours Report*, 14.
90. eSafety Commissioner (2025). How common are experiences of seeing online hate among children in Australia? Accessed 16 June 2026.
91. Kowalski, R.M., Limber, S.P., McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 45.
92. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
93. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
94. FRA (2024). LGBTIQ equality at a crossroads: Progress and challenges, p.72.
95. 5Rights Foundation (2020). Why digital platforms must be designed with LGBTQ children in mind. Accessed on 29 June 2026.
96. Ybarra, M.L., Mitchell, K.J., Palmer, N.A., Reisner, S.L. (2015). Online social support as a buffer against online and offline peer and sexual victimization among U.S. LGBT and non-LGBT youth. *Child Abuse Neglect*, 39.

97. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
98. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
Li, H., Luo, M., Duan, B., Kawulia, A., Su, M., Di, H. (2024). Family socioeconomic status and young children digital addiction: a moderated mediation model. *Frontiers in Psychology*, 27 (5).
99. Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
Gracia, P., Fernandez-Urbano, R., Rubio-Cabañez, M., Celik, S., Cineli, B. (2026). *World Happiness Report 2026, Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries*. Helliwell, J.F., Layard, R., Sachs, J. D., De Neve, J.-E., Aknin, L. B., Wang, S. (editors). Wellbeing Research Centre, University of Oxford.
100. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study. *BMJ Paediatrics Open*, 17:9 (1).
101. Ofcom. (2022). Research into risk factors that may lead children to harm online.
102. Koch, T., Laaber, F., Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behaviour*, 154.
103. World Happiness Report (2026). Chapter 7: Problematic social media use and adolescent wellbeing: the role of family socioeconomic status across 43 countries.
Lu, Z. (2026). Mapping adolescent problematic social media use patterns across 41 countries/ regions: A multilevel latent class analysis with social determinants. *Addictive Behaviors*, 172.
104. Ronis, S., Slaunwhite, A. (2017). Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities Among Youth. *Canadian Journal of Psychology*, 34 (1).
105. Hong, J.S., et al. (2016). Understanding the correlates of face-to-face and cyberbullying victimization among U.S. adolescents: A social-ecological analysis. *Violence and Victims*, 31(4), 638–663.
Thomas, A., Yeqing, L. (2025). Helping teens navigate online racism – study shows which parenting strategy works best.
106. FRA (2023). Online content moderation – Current challenges in detecting hate speech.
107. Bermudez-Villalva, A., Mehrnezhad, M., Toreini, E. (2025). Measuring Online Hate on 4chan using Pre-trained Deep Learning Models. *IEEE Transactions on Technology and Society*, 6 (2), June 2025.
108. FRA (2024). Being Muslim in the EU – Experiences of Muslims.
109. FRA (2023). Being Black in the EU – Experiences of people of African descent.
110. Council of Europe (2026). Hate speech levels across Europe alarming, stronger action needed. Accessed on 25 June 2026.
111. United Nations (2021). Report of the Special Rapporteur on minority issues, Fernand de Varennes. Human Rights Council, Forty-sixth session, 22 February-19 March 2021.
112. FRA (2022). Bias in Algorithms – Artificial Intelligence and Discrimination.
113. Ofcom. (2022). Research into risk factors that may lead children to harm online. p. 27.
114. eSafety Commissioner, 2023. A new playground: The digital lives of young people with disability. Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
115. WeProtect (2025). How do we protect disabled young people from abuse and exploitation in digital spaces?
116. Childlight Global Safety Institute (2023). The nature of online CSEA among children living with disabilities.
117. eSafety Commissioner (2023). Young people with disability more likely to express themselves online despite higher rates of abuse.
118. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.
119. Werling, A.M., Kuzhippallil, S., Emery, S., Walitza, S., Drechsler, R. (2022). Problematic use of digital media in children and adolescents with a diagnosis of attention-deficit/hyperactivity disorder compared to controls. A meta-analysis. *Journal of Behavioral Addictions*, 11 (2).
120. Villar Onrubia, D., Barreda Angeles, M., Cachia, R., Economou, A., Lopez Cobo, M., (2025). Cyberbullying: Insights from science, policy and legislation. Publications Office of the European Union, Luxembourg, JRC144335.
121. Shou, Q., Yamashita, M., Mizuno, Y. (2025). Association of screen time with attention-deficit/hyperactivity disorder symptoms and their development: the mediating role of brain structure. *Translational Psychiatry*, 15:447.
122. eSafety Commissioner (2023). A new playground: The digital lives of young people with disability.

123. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
124. European Commission (2023). Flash Eurobarometer 530: Mental health.
125. World Health Organization (2025). Mental health of adolescents. Accessed on 29 June 2026.
126. World Health Organization (2025). Over a billion people living with mental health conditions – services require urgent scale-up. Accessed on 29 June 2026.
127. World Health Organization (2025). Suicide. Accessed on 16 June 2026:
128. OECD (2021). *Fitter Minds, Fitter Jobs: From Awareness to Change in Integrated Mental Health, Skills and Work Policies*. OECD Publishing, Paris.
129. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
130. Bertoni, E., Centeno, C., Cachia, R. (2025). Social media usage and adolescents' mental health in the EU. European Commission, Joint Research Centre (JRC), Ispra.
131. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). *Minors' health and social media: an interdisciplinary scientific perspective*. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg. P.8.
132. Vidal, C., Lhaksampa, T., Miller, L., Platt, R. (2020). *Social media use and depression in adolescents: A scoping review*. *International Review of Psychiatry* (Abingdon, England), 32(3), 235-253.
133. Prkno, D., Grafe, N., Schulz, M.S., Kiess, W., Poulain, T. (2025). *Children's and adolescents' negative internet experiences and the association with quality of life and behavioural difficulties: a cross-sectional study*. *BMJ Paediatrics Open*, 17;9 (1).
134. Sarmiento, I., Olson, C., Yeo, G., Chen, Y., Toma, C., Brown, B., Bellmore, A., Mares, M. L. (2020). *How does social media use relate to adolescents' internalizing symptoms? Conclusions from a systematic narrative review*. *Adolescent Research Review*, 5, 381-404.
135. Sala, A., Porcaro, L., Gómez, E. (2024). *Social Media Use and adolescents' mental health and well-being: An umbrella review*. *Computers in Human Behavior Reports*, Vol 14. McCrae, N., Gettings, S., Pursell, E. (2017). *Social media and depressive symptoms in childhood and adolescence: A systematic review*. *Adolescent Research Review*, Vol 2, 315-330.
136. Li, H., Zhang, R., Lee, Y.C., et al. (2023). *Systematic review and meta-analysis of AI-based conversational agents for promoting mental health and well-being*. *NPJ Digital Medicine*, 6, 236.
137. Kooli, C., Chakraoui, R. (2025). *AI-driven assistive technologies in inclusive education: benefits, challenges, and policy recommendations*. *Sustainable Futures*, 10.
138. Unicef (2025). Guidance on AI and Children. Accessed on 29 June 2026.
139. Hudon, A., Stip, E. (2025) *Delusional Experiences Emerging From AI Chatbot Interactions or "AI Psychosis"*. *JMIR Mental Health*, 3 (12). European Parliament (2026). The spread of AI companions and the challenges they generate. European Parliamentary Research Service (EPRS). Nature (2025). Can AI chatbots trigger psychosis? What the science says. Accessed on 16 June 2026.
140. Vice (2023). 'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says. Accessed on 16 June 2026.
141. Kurian, N. (2024). *'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models*. *Learning, Media and Technology*, 50.
142. Kurian, N. (2023). *AI's empathy gap: the risks of conversational artificial intelligence for young children's well-being and key ethical considerations for early childhood education and care*. *Contemporary Issues in Early Childhood*, 26(1), 132-139.
143. Commission nationale de l'informatique et des libertés (CNIL) (2026). L'impact des usages de l'AI sur la santé mentale des jeunes européens.
144. Ganapini, M., Panai, E. (2023). An Audit Framework for Adopting AI-Nudging on Children. Tech Ethics Lab.
145. Kurian, N. (2024). *'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models*. *Learning, Media and Technology*, 50.
146. Fegert, J. M. (2026). *European child and adolescent psychiatry in a digital world*. *European Child and Adolescent Psychiatry*, 35, 309–315.
147. Sala, A., Porcaro, L., Gómez, E. (2024). *Social Media Use and adolescents' mental health and well-being: An umbrella review*. *Computers in Human Behavior Reports*, Vol. 14.
148. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). *Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review*. *Frontiers in Psychiatry*, 11.
149. Liu, L. (2024). *Research on the relationship between virtual social interaction and the degree of loneliness based on algorithm matching technologies: A quantitative analysis on the SOUL APP-A virtual social software for strangers*. *PLoS One*, 3:19.

150. eSafety Commissioner (2025). Online risks for children in your community. Accessed on 17 June 2026.
151. 5Rights Foundation (2021). Pathways: How digital design puts children at risk. p.5.
152. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
Bottaro, R., Faraci, P. (2022). The use of social networking sites and its impact on adolescents' emotional well-being: A scoping review. *Current Addiction Reports*, 9, 518–539.
153. Keles, B., McCrae, N., Grealish, A. (2020). A systematic review: The influence of social media on depression, anxiety and psychological distress in adolescents. *International Journal of Adolescence and Youth*, 25 (1), 79–93.
Ivie, E. J., Pettitt, A., Moses, L. J., Allen, N. B. (2020). A meta-analysis of the association between adolescent social media use and depressive symptoms. *Journal of Affective Disorders*, 275, 165–174.
154. Cataldo, I., Lepri, B., Neoh, M. J. Y., Esposito, G. (2021). Social Media Usage and Development of Psychiatric Disorders in Childhood and Adolescence: A Review. *Frontiers in Psychiatry*, 11.
155. Bozzola, E., Spina, G., Agostiniani, R., Barni, S., Russo, R., Scarpato, E., Di Mauro, A., Di Stefano, A. V., Caruso, C., Corsello, G., Staiano, A. (2022). The use of social media in children and adolescents: Scoping review on the potential risks. *International Journal of Environmental Research and Public Health*, 19.
156. Course-Choi, J., Hammond, L. (2021). Social media use and adolescent well-being: A narrative review of longitudinal studies. *Cyberpsychology, Behavior, and Social Networking*, 24, 223–236.
157. Consumer Science and Analytics (2022). Les adolescents et l'info. Research by Milan Presse and YouTube.
Notley, T., Zhong, H.F., Dezuanni, M., et al. (2023) Comparing children's and teens' news engagement practices and affective news experiences. *Journal of Youth Studies*, 26 (7): 878–893.
158. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 25 June 2026.
159. University of Southern Denmark (2025). Children and misinformation on social media. Accessed on 17 June 2026.
160. Calvin, A., Lenhart, A., Mann, S., and Robb, M. (2025). Teens, Trust, and Technology in the Age of AI: Navigating Trust in Online Content. *Common Sense Media*.
161. European Parliament (2025). Youth survey 2024.
162. Ali, S., DiPaola, D., Lee, I., et al. (2021). Children as creators, thinkers and citizens in an AI-driven future. *Computers and Education: Artificial Intelligence*, 2.
163. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
Melchior, C., Oliveira, M. (2024) A systematic literature review of the motivations to share fake news on social media platforms and how to fight them. *New Media and Society*, 26 (2): 1127–1150.
164. Howard, P.N., et al. (2021). Digital Misinformation / disinformation and children. UNICEF.
165. Ma, I., Mubashir, S., Kozyreva, A., van den Bos, W. (2025). Understanding the impact of misinformation on adolescents. *Nature Human Behaviour*, 10, 18–28.
166. NewsGuard (2021). Toxic TikTok: Popular social-media video app feeds vaccine misinformation to kids within minutes after they sign up. Accessed on 17 June 2026.
167. Ludwig-Walz, H., Bujard, M., Fegert, J.M., et al. (2025). Integrating European contexts and needs into WHO guiding principles on online mental health content for young people: Five recommendations. *European Child and Adolescent Psychiatry*, Vol. 34, 1221–1224.
168. Moss, C., Wibberley, C., Witham, G. (2023). Assessing the impact of Instagram use and deliberate self-harm in adolescents: A scoping review. *International Journal of Mental Health Nursing*, 32, 14–29.
169. World Health Organization (2025). Suicide worldwide in 2021: Global health estimates.
170. Arendt, F., Scherr, S., Romer, D. (2019). Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. *New Media and Society*, Vol. 21 (11-12).
Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
171. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
172. Memon, A. M., Sharma, S. G., Mohite, S. S., Jain, S. (2018). The role of online social networking on deliberate self-harm and suicidality in adolescents: A systematized review of literature. *Indian Journal of Psychiatry*, 60 (4).
173. Nesi, J., et al. (2022). Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis. *Clinical Psychology Review*, 8;87.
174. Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. *Manolios*,

- S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.
- 175.** Yue, C., Wenyao, G., Xudong, Y., Shuang, S., Zhuying, S., Yizheng, Z., Linlin, Z., Jinxin, C., Xingqi, W., Yujia, L. (2023). Dose-response relationship between daily screen time and the risk of low back pain among children and adolescents: A meta-analysis of 57831 participants. *Environmental Health and Preventive Medicine*, 28, 64–64.
- 176.** American Optometric Association. (Undated). Computer vision syndrome (Digital eye strain). American Optometric Association. Accessed 29 June 2026.
Thorud, H.-M. S., Aurjord, R., Falkenberg, H. K. (2021). Headache and musculoskeletal pain in school children are associated with uncorrected vision problems and need for glasses: A case-control study. *Scientific Reports*, 11(1).
Thorud, H.-M. S., Mork, R., Bjørset, C. O., Gilson, S. J., Hagen, L. A., Langaas, T., Pedersen, H. R., Svarverud, E., Vikesdal, G. H., Baraas, R. C. (2022). Labouring reading and musculoskeletal pain in school children – the role of lifestyle behaviour and eye wear: A cross-sectional study. *BMC Pediatrics*, 22(1).
Thorud, H.-M. S., Mudvari, P. R., Falkenberg, H. K. (2024). Academic performance and musculoskeletal pain in adolescents with uncorrected vision problems. *BMC Pediatrics*, 24(1).
- 177.** Bozzola, E., Irrera, M., Hellmann, R., Crugliano, S., Fortunato, M. (2024). Media Device Use and Vision Disorders in the Pediatric Age: The State of the Art. *Children (Basel, Switzerland)*, 11(11).
- 178.** Morningstar, B., Clayborne, Z., Wong, S.L., Roberts, K.C., Prince, S.A., Gariépy, G., Goldfield, G.S., Janssen, I., Lang, J.J. (2023). The association between social media use and physical activity among Canadian adolescents: a Health Behaviour in School-aged Children (HBSC) study. *Canadian Journal of Public Health*, 114(4): 642–650.
Foreman, J., Salim, A.T., Praveen, A., Fonseka, D., Ting, D.S.W., Guang He, M., Bourne, R.R.A., Crowston, J., Wong, T.Y., Dirani, M. (2021). Association between digital smart device use and myopia: a systematic review and meta-analysis. *Lancet Digit Health*, 3(12).
Ahmed, O., Walsh, E.I., Dawel, A., Alateeq, K., Espinoza Oyarce, D.A., Cherbuin, N. (2024) Social media use, mental health and sleep: A systematic review with meta-analyses. *Journal of Affective Disorders*, 15;367: 701-712.
Purba, A.K., Thomson, R.M., Henery, P.M., Pearce, A., Henderson, M., Katikireddi, S.V. (2023) Social media use and health risk behaviours in young people: systematic review and meta-analysis. *BMJ*, 383.
- 179.** Czeisler, C. A. (2015). Duration, timing and quality of sleep are each vital for health, performance and safety. *Sleep Health*, 1(1), 5–8.
Matricciani, L., Paquet, C., Galland, B., Short, M., Olds, T. (2019). Children's sleep and health: A meta-review. *Sleep Medicine Reviews*, 46, 136–150.
- Short, M. A., Blunden, S., Rigney, G., Matricciani, L., Coussens, S., M Reynolds, C., Galland, B. (2018). Cognition and objectively measured sleep duration in children: A systematic review and meta-analysis. *Sleep Health*, 4(3), 292–300.
- 180.** Wheaton, A. G., Claussen, A. H. (2021). Short Sleep Duration Among Infants, Children, and Adolescents Aged 4 Months-17 Years – United States, 2016-2018. *MMWR. Morbidity and Mortality Weekly Report*, 70(38).
Gariépy, G., et al. (2020). How Are Adolescents Sleeping? Adolescent Sleep Patterns and Sociodemographic Differences in 24 European and North American Countries. *Journal of Adolescent Health*, 66 (6) Supplement.
- 181.** Chang, A.M., Aeschbach, D., Duffy, J. F., Czeisler, C. A. (2015). Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness. *Proceedings of the National Academy of Sciences*, 112(4), 1232–1237.
Hale, L., Guan, S. (2015). Screen time and sleep among school-aged children and adolescents: A systematic literature review. *Sleep Medicine Reviews*, 21, 50–58.
- 182.** Tähkämö, L., Partonen, T., Pesonen, A.K. (2019). Systematic review of light exposure impact on human circadian rhythm. *Chronobiology International*, 36(2): 151-170.
- 183.** Lund, L., Sølvhøj, I. N., Danielsen, D., Andersen, S. (2021). Electronic media use and sleep in children and adolescents in western countries: A systematic review. *BMC Public Health*, 21(1), 1598.
- 184.** Mammeri, K., Riontino, L., Schwartz, S., Sterpenich, V. (2025). Influence of parental rules about screen electronic device use in the evening on sleep in adolescents. *Discover Public Health*, 22:517
- 185.** Perrault, A. A., Bayer, L., Peuvrier, M., Afyouni, A., Ghisletta, P., Brockmann, C., Spiridon, M., Hulo Vesely, S., Haller, D. M., Pichon, S., Perrig, S., Schwartz, S., Sterpenich, V. (2019). Reducing the use of screen electronic devices in the evening is associated with improved sleep and daytime vigilance in adolescents. *Sleep*, 42(9).
Bartel, K., Scheeren, R., Gradisar, M. (2019). Altering Adolescents' Pre-Bedtime Phone Use to Achieve Better Sleep Health. *Health Communication*, 34(4), 456–462.
- 186.** World Health Organization. Regional Office for Europe (2024) A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey.
- 187.** Digital Services Act.
- 188.** European Commission (2023). Consumer protection: manipulative online practices found on 148 out of 399 online shops screened.

189. Flayelle, M., et al. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology*, 2: 136–150.
Perales, J.C., et al. (2020). Learning to lose control: A process-based account of behavioral addiction. *Neuroscience and biobehavioural reviews*, 108: 771–780.
190. van der Wal, A., Beyens, I., Janssen, L.H.C., Valkenburg, P.M. (2025). Diverse platforms, diverse effects: Evidence from a 100-day study on social media and adolescent mental health. *Current Psychology*, 45 (36).
191. Owenz, M., Freed, R. (2021). The ethics of persuasive design in technology used by children and adolescents. *Ethical Human Psychology Psychiatry*, 23, 89–99.
192. Andreassen, C.S., et al. (2016). The Relationship between Addictive Use of Social Media and Video Games and Symptoms of Psychiatric Disorders: A Large-Scale Cross-Sectional Study. *Psychology of Addictive Behaviors*. 30(2): 252–62.
193. European Commission (2024). Commission Staff Working Document Fitness Check on EU consumer law on digital fairness.
194. Saura, J.R., Palacios-Marqués, D., Iturricha-Fernández, A. (2021). Ethical design in social media: Assessing the main performance measurements of user online behavior modification. *Journal of Business Research*, 129.
195. United Nations (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Committee on the Rights of the Child.
European Commission (2025). Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065.
196. Curtis, B. L., Lookatch, S. J., Ramo, D. E., McKay, J. R., Feinn, R. S., Kranzler, H. R. (2018). Meta-Analysis of the Association of Alcohol-Related Social Media Use with Alcohol Consumption and Alcohol-Related Problems in Adolescents and Young Adults. *Alcoholism: Clinical and Experimental Research*, 42(6), 978–986.
Vannucci, A., Simpson, E. G., Gagnon, S., Ohannessian, C. M. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence*, 79(1), 258–274.
197. Beullens, K., Schepers, A. (2013). Display of alcohol use on Facebook: A content analysis. *Cyberpsychology, Behavior and Social Networking*, 16(7), 497–503.
Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
Vranken, S., Kurten, S., Beullens, K. (2024). Time to 'Wine': A Content Analysis Investigating How Social Media Influencers Refer to Alcohol Use in Instagram's Feed Posts and Stories. *Mass Communication and Society*, 27(6), 1468–1494.
198. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216. Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791.
Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
199. Geusens, F., Beullens, K. (2018). The Association Between Social Networking Sites and Alcohol Abuse Among Belgian Adolescents: The Role of Attitudes and Social Norms. *Journal of Media Psychology*, 30(4), 207–216.
Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297.
Geusens, F., Beullens, K. (2021). Triple spirals? A three-wave panel study on the longitudinal associations between social media use and young individuals' alcohol consumption. *Media Psychology*, 24(6), 766–791.
Vanherle, R., Hendriks, H., Beullens, K. (2023). Only for Friends, Definitely Not for Parents: Adolescents' Sharing of Alcohol References on Social Media Features. *Mass Communication and Society*, 26(1), 47–73.
200. Geusens, F., Beullens, K. (2019). A Longitudinal Examination of the Moderating Influence of Peer and Parental Socialization on Alcohol-Related Social Media Self-Effects Among Late Adolescents. *Media Psychology*, 22(2), 273–297.
201. Rutherford, B.N., et al. (2025). #TurntTrending: a systematic review of substance use portrayals on social media platforms. *Addiction*, 8;118 (2).
202. Liu, J., Charmaraman, L., Bickham, D. (2024). Association between social media use and substance use among middle and high school-aged youth. *Substance Use and Misuse*, 59 (7).
203. Europol (2025). Europol coordinates operation against terrorist content online targeting minors. Accessed on 29 June 2026.
204. Europol (2026). 2025 Serious and Organised Crime Threat Assessment (SOCTA): The changing DNA of serious and organised crime.
205. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). EU Kids Online 2020: Survey results from

- 19 countries. EU Kids Online. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
- 206.** Chauviré-Geib, K., et al. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full picture. *Child Abuse and Neglect*, 164. Dreßing, H., Hoell, A., Scharmann, L., Simon, A. M., Haag, A. C., Dölling, D., Meyer-Lindenberg, A., Fegert, J. M. (2025). Sexual Violence Against Children and Adolescents: A German Nationwide Representative Survey on Its Prevalence, Situational Context, and Consequences. *Deutsches Ärzteblatt International*, 122(11), 285.
- 207.** Internet Watch Foundation (2026). 2025 Internet Watch Foundation Annual Data and Insights Report.
- 208.** Insoll, T., Ovaska, A., Vaaranen-Valkonen, N. (2024). CSAM Users in the Dark Web: Protecting Children Through Prevention. *Protect Children*.
- 209.** Internet Watch Foundation (2026). 2025 Internet Watch Foundation Annual Data and Insights Report.
- 210.** Our Voice (2025) Survey for survivors of sexual violence in childhood – voices of the Nordic survivors.
- 211.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
- 212.** Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
- 213.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
- 214.** Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
- 215.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4).
- Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
- 216.** Haag, A. C., Bonanno, G. A., Chen, S., Herd, T., Strong-Jones, S., S. S., Noll, J. G. (2023). Understanding posttraumatic stress trajectories in adolescent females: A strength-based machine learning approach examining risk and protective factors including online behaviors. *Development and Psychopathology*, 35 (4). Chauviré-Geib, K., Fegert, J. M. (2023). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, 25(2).
- 217.** Chauviré-Geib, K., Gerke, J., Haag, A. C., Sachser, C., Finkelhor, D., Rassenhofer, M., Fegert, J. M. (2025). The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. *Child Abuse Neglect*, 164.
- 218.** Eurostat (2025). EU Terrorism Situation and Trend Report.
- 219.** Krahé, B., Möller, I., Huesmann, L.R., Kirwil, L., Felber, J., Berger, A. (2011). Desensitization to Media Violence: Links With Habitual Media Violence Exposure, Aggressive Cognitions, and Aggressive Behavior. *Journal of Personality and Social Psychology*, 100(4).
- 220.** Article 17 GDPR.
- 221.** European Data Protection Board (2022). Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.
- 222.** Schlegel, L., (2022). Playing Against Radicalization: Why extremists are gaming and how P/CVE can leverage the positive effects of video games to prevent radicalization.
- 223.** European Commission (2023). Understanding the value of a European video games society – Final report. Directorate-General for Communications Networks, Content and Technology (DG CNECT), ECORYS and KEA, section. 5.1.2. Kowert, R., et al. (2026). Editorial: Extremism in games. *Frontiers in Psychology*, Vol. 16, p. 12.
- 224.** European Commission (2025). The European media industry outlook – September 2025. Directorate-General for Communications Networks, Content and Technology (DG CNECT), p. 99.
- 225.** Radicalisation Awareness Network (2021). Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities – Conclusion paper.
- 226.** Brooks, G.A., Clark, L. (2019). Associations between loot box use, problematic gaming and gambling, and gambling-related cognitions. *Addictive Behaviors*, 96.
- 227.** Boniel-Nissim, M., Marino, C., Galeotti, T., Blinka, L., Ozoliņa, K., Craig, W., et al. (2024). A focus on adolescent social media use and gaming in Europe.

- central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey. Volume 6. WHO Regional Office for Europe.
- 228.** PEGI (2026). PEGI expands age rating criteria with interactive risk categories. Accessed on 17 June 2026.
- 229.** OECD (2021). Children in the digital environment – Revised typology of risks.
- 230.** Livingstone, S., Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children (1.0.0).
- 231.** European Commission, Joint Research Centre
- 232.** Beullens, K., Bozzola, E., Cataldo, I., Hale, L., Kent, M., Montag, C., Nivins, S., O'reilly, M., Rubæk, L., Schiøtz Thorud, H.-M., Sterpenich, V., Vandenbosch, L. (2025). Minors' health and social media: an interdisciplinary scientific perspective. Manolios, S., Sala, A., Sundorph, E., Chaudron, S., Gomez, E. (editors), Publications Office of the European Union, Luxembourg.
- 233.** Bursztyn, L., Duckworth, A., JiménezDurán, R., Leonard, A., Milojević, F., Roth, C., Sunstein, C. R. (2026). Why bans fail: Tipping points and Australia's socialmedia ban. (BFI Working Paper No. 202657). Becker Friedman Institute for Economics.
- 234.** Article 28 DSA.
- 235.** Articles 34 and 35 DSA.
- 236.** Article 25 GDPR.
- 237.** Article 6(1) GDPR.
- 238.** Article 4(11) GDPR.
- 239.** EDPB Guidelines 05/2020 on consent under Regulation 2016/679, pp. 62.
- 240.** Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 106.
- 241.** CJEU C-252/21 Bundeskartellamt, paragraph 111.
- 242.** EDPB guidelines on legitimate interest, para 96.
- 243.** EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, §54. Case C-252/21, Meta v. Bundeskartellamt (ECLI:EU:C:2023:537), paragraph 111.
- 244.** EDPB Guidelines 8/2020 on the targeting of social media users, paragraph 16.
- 245.** EDPB guidelines on legitimate interest, paragraph 95.
- 246.** Article 17 and recital 65 GDPR.
- 247.** Article 22 and recital 71 GDPR.
- 248.** Recital 38 GDPR.
- 249.** Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
- 250.** Article 35 and 36 GDPR.
- 251.** European Commission (2026). Draft Commission guidelines on the classification of high-risk AI systems.
- 252.** European Commission (2025). Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act. Accessed on 2 July 2026.
- 253.** European Commission (2026). The General-Purpose AI Code of Practice.
- 254.** Article 50 AI Act.
- 255.** European Commission (2026). Code of Practice on marking and labelling of AI-generated content.
- 256.** European Commission (2026). Draft of the guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act.
- 257.** European Commission (2021). UCPD Guidelines.
- 258.** Digital Fairness Fitness Check
- 259.** European Commission (2026). Action Plan against Cyberbullying.
- 260.** European Commission (2024). Commission Recommendation on developing and strengthening integrated child protection systems in the best interests of the child.
- 261.** European Commission (2024). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act. Accessed on 2 July 2026.
- 262.** Article 82 DSA.
- 263.** European Commission (2026). Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act. Accessed on 2 July 2026.
- 264.** European Commission (2026). Commission preliminarily finds Pornhub, Stripchat, XNXX and XVideos in breach of the Digital Services Act for allowing minors to access their services. Accessed on 2 July 2026.
- 265.** European Commission (2025). The European Board for Digital Services launches a coordinated action to reinforce the protection of minors as regards pornographic platforms. Accessed on 2 July 2026.
- 266.** European Commission (2026). Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook. Accessed on 2 July 2026.
- 267.** European Commission (2026). Commission investigates Snapchat's compliance with child protection rules under the Digital Services. Accessed on 2 July 2026.

268. European Commission (2025). Commission accepts commitments offered by AliExpress under the DSA and takes further action. Accessed on 2 July 2026. European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026. European Commission (2025). Commission preliminarily finds Temu in breach of the Digital Services Act. Accessed on 2 July 2026.
269. Authority for Consumers and Markets (2026). ACM launches investigation into Roblox in connection with risks that minors are facing. Accessed on 2 July 2026.
270. European Commission (2026). Commission investigates Grok and X's recommender systems under the Digital Services Act. Accessed on 2 July 2026.
271. European Commission (2026). Commission launches investigation into Shein under the Digital Services Act. Accessed on 2 July 2026.
272. European Commission (2024). Commission opens formal proceedings against Temu under the Digital Services Act. Accessed on 2 July 2026.
273. Article 53 AI Act.
274. Article 55 AI Act.
275. DLA Piper (2026). DLA Piper GDPR Fines and Data Breach Survey: January 2026.
276. Data Protection Commission (2023). Annual Report 2023.
277. Data Protection Commission (2023). Irish Data Protection Commission announces €345 million fine of TikTok. Accessed on 2 July 2026.
278. Data Protection Commission (2022). Data Protection Commission announces decision in Instagram Inquiry. Accessed on 2 July 2026.
279. Garante per la Protezione dei Dati Personali (2021). Provvedimento del 22 gennaio 2021.
280. Data Protection Commission (2026). Data Protection Commission opens investigation into X (XIUC). Accessed on 2 July 2026.
281. Art 15 EMFA.
282. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
283. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
284. European Commission (undated). Sweeps. Accessed on 24 June 2026.
285. European Commission (undated). Influencer Legal Hub. Accessed on 24 June 2026.
286. European Commission (undated). Social media, online games and search engines. Accessed on 24 June 2026.
287. Article 37 DSA.
288. Article 38 DSA.
289. FRA (2025). Towards Integrated Child Protection Systems – Challenges, promising practices and ways forward, p.79.
290. Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
291. Singleton, A., Abeles, P., Smith, I.C. (2016). Online social networking and psychological experiences: The perceptions of young people with mental health difficulties. Computers in Human Behavior, vol. 61.
292. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
293. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
294. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
295. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
296. Anderson, M., Vogels, E.A., Perrin, A., Lee, R. (2022). Connection, Creativity and Drama: Teen Life on Social Media in 2022. Pew Research Center. As cited in: Manolios, S., Chaudron, S., Fortuna, P., Sala, A., Gomez, E. (2026). Opportunities for young users on social media. European Commission, Joint Research Centre (JRC), Seville, JRC147510.
297. Sala, A., Porcaro, L., and Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. Computers in Human Behavior Reports, vol. 14, p. 8.
298. Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
299. Shankleman, M., Hammond, L., Jones, F.W. (2021). Adolescent Social Media Use and Well-Being: A Systematic Review and Thematic Meta-synthesis. Adolescent Research Review, vol. 6.
300. Popat, A., Tarrant, C. (2023). Exploring adolescents' perspectives on social media and mental health and

- well-being – A qualitative literature review. Special Issue: Social Media and Mental Health, 28 (1), p. 329.
- 301.** Hillmayr, D., Ziernwald, L., Reinhold, F., Hofer, S.I., Reiss, K.M. (2020). The potential of digital tools to enhance mathematics and science learning in secondary schools: A context-specific meta-analysis. *Computers & Education*, vol. 153.
- 302.** Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. *Education and Information Technologies*, vol. 28.
- 303.** Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. *OECD Education Working Paper No. 336*.
Barrot, J.S. (2022). Social media as a language learning environment: A systematic review of the literature (2008-2019). *Computer Assisted Language Learning*, 35 (9).
Zachos, G., Paraskevopoulou-Kollia, E.-A., Anagnostopoulos, I. (2018). Social Media Use in Higher Education: A Review. *Education Sciences*, 8 (4), Article 4.
- 304.** Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. *OECD Education Working Paper No. 336*.
- 305.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
Forsström, S., Njå, M., Munthe, E., Houldsworth, L., Álvarez-Galván, J.-L. (2025). Key findings and integration strategies on the impact of digital technologies on students' learning: Results from a literature review. *OECD Education Working Paper No. 336*.
- 306.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al. (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 307.** Villar Onrubia, D., Cachia, R., Rietz, C., Feltrero, R., Niemi, H. et al., (2025). Generative Artificial Intelligence in secondary education – Uses and perceptions from the perspective of early adopters across five EU Member States. Luxembourg, JRC144345.
- 308.** Timotheou, S., Miliou, O., Dimitriadis, Y., Villagrà Sobrino, S., Giannoutsou, N., Cachia, R., Martínez Monés, A., Ioannou, A. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. *Education and Information Technologies*, vol. 28.
- 309.** Crêteur, S., Dunajeva, J., Frydman, B., Berg Mulvik, I., Del Cogliano, D., Nada, C., Siarova, H., Sankalaite, S. (2026). Mobile phone bans in schools across the EU: ENESET analytical report. European Commission, Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 310.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 311.** European Commission (2026). Better Internet for Kids: Review of the year 2025. Accessed on 2 July 2026.
- 312.** European Commission (2024). International Computer and Information Literacy Study (ICILS) in Europe, 2023: Main findings and educational policy implications. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 313.** European Commission (2025). Education and Training Monitor: Comparative Report. Chapter 2 – Young people's basic skills.
- 314.** European Commission (2026). The teaching profession in the EU – A comparative analysis building upon the TALIS 2024 results. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 315.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 316.** COFACE Families Europe (2026). Towards digital safety and well-being for children and their families: Moving beyond social media age restrictions as the sole solution.
- 317.** Council conclusions on promoting and protecting the mental health of children and adolescents in the digital era.
- 318.** European Commission (2025). Flash Eurobarometer survey: Future needs in digital education.
- 319.** European Commission (2026). New guidelines to help teachers lead Europe's digital education. Accessed on 1 July 2026.
- 320.** European Commission (2026). Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training. Directorate-General for Education, Youth, Sport and Culture (DG EAC).
- 321.** OECD / European Union (2026). Empowering Learners for the Age of AI: An AI Literacy Framework

for Primary and Secondary Education. OECD Publishing, Paris.

- 322.** Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child.
- 323.** Article 24 Charter of Fundamental Rights of the European Union.
- 324.** European Commission (2025). Call to Action: from children to EU decision-makers. Accessed on 1 July 2026.
- 325.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 326.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 327.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 328.** O'Connell, R. (2021). Psychological first aid for Young Peers. Training manual. IFRC Reference Centre for Psychosocial Support, Copenhagen.
- 329.** European Commission (Undated). Promising practices – Summary. Denmark – Psychological First Aid for Young Peers.
- 330.** European Commission (2024). Best Practices Portal – Psychological First Aid for Young Peers. Accessed on 1 July 2026.
- 331.** Seguranet (2026) Digital Leaders | SeguraNet. Accessed on 7 July 2026.



**Oficina de Publicaciones
de la Unión Europea**

Derecho | Datos | Publicaciones