

Rad. 2026201704
Cod. 11000
Bogotá, D.C.

Radicado:	2026533632
Fecha:	6/10/2026 10:29:18 A. M.
Proceso:	11000 PROSPECTIVA ESTRATÉGICA E INNOVACI
Destino:	CONGRESO DE LA REPÚBLICA DE COLOMBIA
Asunto:	OBSERVACIONES AL PROYECTO DE LEY NO. 054 DE 2026 SENADO

Honorables Senadores

ENRIQUE CABRALES BAQUERO
HERNÁN DARÍO CADAVID MÁRQUEZ
CONGRESO DE LA REPÚBLICA DE COLOMBIA

Correos electrónicos: enrique.cabral@senado.gov.co; hernan.cadavid@senado.gov.co ;
comision.primer@senado.gov.co

Ciudad

REF: Observaciones al Proyecto de Ley No. 054 de 2026 Senado «Por medio del cual se establecen medidas de protección digital reforzada" para los niños, niñas y adolescentes, se prohíbe el acceso a redes sociales digitales y se dictan otras disposiciones».

Honorables Senadores:

La Comisión de Regulación de Comunicaciones (CRC) se permite presentar las siguientes observaciones al Proyecto de Ley No. 054 de 2026 Senado, «Por medio del cual se establecen medidas de protección digital reforzada para los niños, niñas y adolescentes, se prohíbe el acceso a redes sociales digitales y se dictan otras disposiciones», actualmente en trámite ante el Congreso de la República.

El Proyecto de Ley 054 de 2026¹ tiene como objeto prohibir el acceso a redes sociales a menores de 16 años y obligar a las plataformas a implementar mecanismos robustos de verificación, así como prevenir evasiones y eliminar cuentas de menores. El proyecto busca proteger a niños, niñas y adolescentes del tratamiento masivo de datos, el perfilamiento algorítmico, la recomendación automatizada y funcionalidades diseñadas para prolongar intensivamente su permanencia e interacción. Esto imponiendo a las plataformas la adopción de programas internos de cumplimiento, conservación de evidencias, informes periódicos, cooperación con las autoridades y auditorías sobre los mecanismos adoptados. En adición, asigna a la Superintendencia de Industria y Comercio facultades de vigilancia, auditoría, imposición de medidas cautelares, suspensión de funcionalidades y sanciones por incumplimiento y distribuye responsabilidades entre Estado, familias, sociedad y plataformas, ordenando reglamentar una política de uso seguro, responsable e informado de las tecnologías dirigida a padres y cuidadores.

¹ Gaceta del Congreso No.976 del 11 de agosto de 2026.

En el marco de las competencias asignadas a esta Comisión por la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, la CRC considera pertinente aportar al análisis legislativo elementos técnicos, económicos y regulatorios relacionados con la protección de los niños, niñas y adolescentes en los entornos digitales. Las observaciones se concentran en la proporcionalidad y efectividad de las medidas propuestas, su viabilidad técnica, su articulación con el marco normativo vigente y las condiciones necesarias para verificar posteriormente sus resultados.

La protección de los niños, niñas y adolescentes frente a los riesgos presentes en los entornos digitales constituye el propósito común de las medidas analizadas. Desde una perspectiva regulatoria, el desafío consiste en identificar con precisión los riesgos que justifican una intervención, los actores que tienen capacidad efectiva para prevenirlos o mitigarlos y los instrumentos que pueden reducirlos de manera verificable, procurando preservar los demás derechos e intereses legítimos involucrados.

Este análisis resulta especialmente relevante en entornos caracterizados por asimetrías de información y diferencias importantes en la capacidad de controlar las fuentes del riesgo. Las plataformas diseñan y administran aspectos esenciales del funcionamiento de sus servicios — incluidos los sistemas de recomendación, las formas de interacción entre usuarios, las configuraciones predeterminadas y el tratamiento de información—, mientras que los usuarios y sus familias no necesariamente disponen de información equivalente sobre su funcionamiento, sus efectos o las alternativas disponibles para gestionarlos. Asimismo, determinadas decisiones de diseño pueden generar beneficios para quien presta el servicio mientras parte de los riesgos asociados recaen sobre los usuarios. Estas condiciones pueden justificar obligaciones de transparencia, prevención, diseño seguro y gestión de riesgos, pero no determinan por sí mismas la naturaleza ni la intensidad de la intervención regulatoria.

Por esta razón, las observaciones que se presentan a continuación examinan el contenido del articulado a partir de su relación con el marco normativo vigente —en particular con la Ley 2489 de 2025 y su reglamentación—, la evidencia y experiencias internacionales disponibles y las condiciones concretas de implementación de las medidas propuestas. El análisis considera, entre otros aspectos, la correspondencia entre la intensidad de cada obligación y el riesgo que pretende mitigar, la capacidad real de los sujetos obligados para incidir sobre dicho riesgo, la existencia de alternativas menos intensivas, los costos de cumplimiento y supervisión, la posibilidad de evasión o desplazamiento hacia otros servicios y la existencia de indicadores que permitan verificar su efectividad.

Bajo este enfoque, la valoración regulatoria no se agota en determinar si una medida persigue una finalidad legítima, sino también en establecer si puede producir un beneficio adicional y verificable frente a los instrumentos existentes, si dicho beneficio guarda relación con los costos y riesgos que introduce y si su diseño permite adaptarse a la evolución tecnológica. El objetivo es aportar elementos que contribuyan a fortalecer la iniciativa y favorecer un marco normativo articulado, técnicamente viable, basado en evidencia y orientado a una reducción efectiva y sostenible de los riesgos que enfrentan los niños, niñas y adolescentes en los entornos digitales. Este enfoque supone diferenciar el objetivo legítimo de protección de los instrumentos utilizados para alcanzarlo

y valorar, para cada uno de ellos, tanto los beneficios esperados como las eventuales afectaciones sobre otros derechos, los incentivos que genera y sus posibles efectos no previstos.

Antes de exponer las líneas de comentarios específicos de la CRC respecto del proyecto de ley, resulta pertinente considerar los resultados disponibles sobre medidas similares en el resto del mundo.

1. Experiencia internacional y evidencia relevante para el análisis legislativo

La protección de los niños, niñas y adolescentes en los entornos digitales ha dado lugar a respuestas de distinta naturaleza e intensidad. Algunas intervienen sobre el diseño y funcionamiento de los servicios; otras incorporan mecanismos de garantía de edad, participación parental, restricciones sobre determinadas funcionalidades o límites de acceso. Esta variedad responde, en parte, a que los riesgos tampoco son homogéneos: pueden provenir del contenido al que se expone el menor, de la interacción con otros usuarios, de determinadas características del diseño del servicio o de la manera en que estas dimensiones se combinan.

Esta variedad ofrece elementos útiles para examinar el Proyecto de Ley, particularmente en relación con cinco aspectos: (i) la correspondencia entre los riesgos identificados y las medidas previstas; (ii) la función que cumple la garantía de edad dentro de cada esquema; (iii) las condiciones técnicas necesarias para su implementación; (iv) la evidencia disponible sobre los resultados alcanzados; y (v) las garantías que han acompañado medidas de mayor intensidad.

La evidencia disponible permite, al mismo tiempo, precisar el alcance de esa revisión. Existen riesgos asociados con determinadas formas de uso de redes sociales y otros servicios digitales que justifican medidas de protección. Sin embargo, su magnitud no aparece distribuida de manera uniforme entre todos los menores ni todos los usos, y continúa abierta la discusión sobre los mecanismos mediante los cuales se producen algunos de esos efectos. También existe evidencia de que determinadas intervenciones pueden modificar el comportamiento, el bienestar o el aprendizaje, aunque sus resultados varían según el contexto y la medida aplicada. Finalmente, la experiencia australiana ofrece una oportunidad todavía reciente para observar qué ocurre cuando una restricción general por edad se convierte efectivamente en política pública.

Por esta razón, al abordar el cuarto de los aspectos señalados —la evidencia sobre resultados— conviene distinguir tres preguntas que no necesariamente tienen la misma respuesta: ¿qué sabemos sobre los riesgos y su distribución entre diferentes usuarios y formas de uso?; ¿qué ocurre cuando se interviene sobre determinadas prácticas o funcionalidades?; y ¿qué resultados produce una restricción general por edad cuando se implementa a escala nacional? Esta distinción permite valorar las alternativas previstas en la iniciativa sin asumir que la existencia de un riesgo determina por sí sola el instrumento más adecuado para reducirlo.

1.1. Diferentes instrumentos frente a diferentes fuentes de riesgo

Para los niños, niñas y adolescentes, los entornos digitales forman parte de los espacios en los que hoy se informan, aprenden, se expresan, crean y se relacionan con otros. Esa presencia cada vez

más cotidiana también puede exponerlos a riesgos asociados con los contenidos que reciben, las personas con quienes interactúan y la manera en que están diseñados y funcionan los servicios que utilizan. El marco europeo parte de esa realidad y combina distintas medidas de protección, en lugar de concentrarlas exclusivamente en una condición de acceso².

Las Directrices adoptadas por la Comisión Europea en desarrollo del artículo 28 del Reglamento de Servicios Digitales contemplan, entre otras medidas, configuraciones de privacidad y seguridad adecuadas para menores, condiciones aplicables a los sistemas de recomendación, herramientas para gestionar el contacto con otros usuarios y mecanismos de garantía de edad. En materia de recomendación, por ejemplo, consideran el grupo etario, las necesidades y el grado de desarrollo de los menores y contemplan opciones para ejercer mayor control sobre los contenidos recomendados y limitar determinadas formas de perfilamiento.

El panorama comparado muestra que las restricciones de edad no responden a un único modelo regulatorio. A abril de 2026, la OCDE registraba 25 países miembros o candidatos con restricciones de edad para redes sociales vigentes, aprobadas o en consideración; sin embargo, solo Australia, Brasil e Indonesia contaban con leyes en vigor, mientras los demás casos se encontraban en fase de propuesta o consulta³. Esa heterogeneidad no es solo jurídica, sino también funcional, la garantía de edad no se limita a redes sociales. La OCDE ha examinado prácticas de garantía de edad en cincuenta servicios usados por niños, pertenecientes a diez categorías distintas, incluidas redes sociales, mensajería, videojuegos, tiendas de aplicaciones, videochat aleatorio, inteligencia artificial generativa, pornografía y entornos inmersivos⁴. Esto confirma que cualquier medida debe precisar con claridad qué servicios cubre, qué riesgo busca corregir y qué mecanismo técnico hará exigible la restricción.

Estos antecedentes muestran que el análisis legislativo puede beneficiarse de una aproximación que no dependa únicamente de la categoría jurídica o comercial del servicio. Funcionalidades semejantes pueden encontrarse en servicios distintos y, a su vez, servicios comprendidos bajo una misma denominación pueden presentar riesgos diferentes para los menores. En ese contexto, podría resultar útil valorar de manera conjunta la naturaleza del riesgo, la funcionalidad a través de la cual se materializa, el grupo etario involucrado y el tipo de medida prevista para atenderlo.

1.2. La garantía de edad y las condiciones para su implementación

La garantía de edad permite determinar si a un usuario le resultan aplicables determinadas condiciones de acceso o protección. Su función es distinta de las medidas que actúan directamente sobre el diseño y funcionamiento del servicio. Una plataforma podría identificar correctamente que

² COMISIÓN EUROPEA. Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065. Comunicación C/2025/5519, Diario Oficial de la Unión Europea, 10 de octubre de 2025.

³ OCDE. *Social media age restrictions for children: Why they are rising and what comes next*. 14 de abril de 2026. <https://www.oecd.org/en/blogs/2026/04/social-media-age-restrictions-for-children-why-they-are-rising-and-what-comes-next.html>

⁴ OCDE. *Age Assurance Practices of 50 Online Services Used by Children*. OECD Publishing, París, 25 de junio de 2025. DOI 10.1787/a19853ab-en

un usuario es menor y mantener, al mismo tiempo, funcionalidades asociadas con sistemas de recomendación, contacto con terceros, geolocalización, publicidad o difusión de contenidos que requieran medidas adicionales de protección.

La práctica observada por la OCDE muestra, además, una diferencia importante entre establecer formalmente una edad mínima y contar con mecanismos para aplicarla. De los cincuenta servicios estudiados, veintiocho —56%— utilizaban algún mecanismo de garantía de edad, mientras únicamente dos lo aplicaban sistemáticamente al momento de creación de una cuenta. El informe también encontró servicios con edades mínimas declaradas que no utilizaban mecanismos para comprobarlas de manera general. La información pública sobre el desempeño de estos mecanismos era igualmente limitada. Solo tres servicios incluían en sus reportes de transparencia información sobre la ejecución de sus políticas de edad y apenas uno reportaba información sobre la eficacia del mecanismo utilizado⁵. Para el análisis legislativo, esta diferencia puede ser relevante porque permite separar la existencia formal de una obligación de las condiciones necesarias para verificar posteriormente su cumplimiento y efectividad.

La experiencia británica aporta otro elemento. Ofcom ha señalado que los métodos de garantía de edad ofrecen niveles diferentes de certeza y operan en momentos distintos de la relación con el usuario. Por ejemplo, un mecanismo que estima la edad a partir de la forma en que una persona utiliza el servicio solo puede funcionar después de que ese usuario haya generado suficiente información sobre su comportamiento. Por tanto, puede resultar útil para detectar posteriormente posibles inconsistencias en la edad declarada o activar protecciones adicionales durante el uso, pero no necesariamente para impedir desde el inicio la creación de una cuenta. Ofcom también ha advertido que ningún método elimina por sí solo todas las posibilidades de evasión y ha considerado la conveniencia de combinar distintas capas de protección⁶.

Cuando la regla pretende impedir el acceso desde el inicio, pueden resultar relevantes no solo la precisión del mecanismo, sino también el momento en que produce la decisión, sus tasas de error, su resistencia a la evasión y la posibilidad de corregir una clasificación equivocada.

La cantidad de información necesaria para alcanzar determinado grado de certeza introduce otra consideración. Algunos métodos utilizan documentos, atributos provenientes de terceros, biometría u otras fuentes de información personal. Las Directrices europeas vinculan por ello la garantía de edad con los principios de privacidad desde el diseño y minimización de datos.⁷

La arquitectura desarrollada por la Comisión Europea muestra que acreditar una edad no exige necesariamente comunicar la identidad completa del usuario a cada servicio. El *blueprint* europeo está diseñado para que una fuente confiable realice la comprobación y posteriormente pueda

⁵ Ibidem.

⁶ OFCOM. Protecting Children from Harms Online. Volume 4 – What Should Services Do to Mitigate the Risks of Online Harms to Children, 2025, párrs. 9.70–9.73; y Use of Age Assurance Report 2026, 15 de julio de 2026, actualizado el 27 de julio de 2026.

⁷ COMISIÓN EUROPEA. Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065. Comunicación C/2025/5519, Diario Oficial de la Unión Europea, 10 de octubre de 2025.

acreditarse ante el servicio únicamente que la persona supera determinado umbral, reduciendo la información de identificación que recibe quien presta el servicio⁸.

El ejemplo europeo permite ilustrar una distinción útil para la discusión legislativa. Si la finalidad de la medida consiste únicamente en comprobar que una persona supera determinado umbral de edad, esa comprobación puede diseñarse sin que la plataforma conozca necesariamente su identidad completa. Además, si para aplicar la medida se requiere identificar a la persona, la necesidad de recopilar esa información responde a una finalidad adicional que convendría justificar de manera específica. Así, más que predeterminar desde la ley una tecnología concreta, el análisis puede considerar qué información necesita realmente el sujeto obligado para cumplir la medida y qué garantías deben acompañar su tratamiento.

1.3. Evidencia sobre riesgos, heterogeneidad e intervención

La evidencia empírica puede examinarse desde tres planos complementarios. El primero se refiere a los efectos asociados al uso de redes sociales y otros servicios digitales y a su distribución entre usuarios y formas de uso. El segundo observa qué ocurre cuando se modifica experimentalmente o mediante políticas específicas la manera en que las personas utilizan esas tecnologías. El tercero permite estudiar los primeros resultados de una restricción general por edad implementada a escala nacional. Cada plano responde una pregunta distinta y ofrece información diferente para la discusión legislativa.

1.3.1. Riesgos, salud mental y heterogeneidad de los efectos

La literatura sobre redes sociales, tecnologías digitales y bienestar no conduce a una estimación única del efecto. Una parte de las diferencias proviene de la población estudiada y otra de la manera en que se define y mide la exposición.

Orben y Przybylski analizaron tres grandes bases de datos que, en conjunto, comprendían 355.358 adolescentes. Encontraron una asociación negativa entre uso agregado de tecnologías digitales y bienestar, pero de magnitud reducida con una variación máxima sobre el bienestar de 0,4%⁹. El propio trabajo advierte que esos resultados no permiten establecer si un mayor uso produce menor bienestar, si un menor bienestar conduce a mayor uso o si otros factores explican ambas circunstancias. El aporte del estudio para esta discusión es también metodológico, pues muestra que el resultado puede cambiar de manera importante según cómo se definan el uso digital, el bienestar y las variables de control. Las consideraciones metodológicas expuestas no permiten que

⁸ COMISIÓN EUROPEA. Blueprint for an Age Verification Solution to Help Protect Minors Online. Shaping Europe's Digital Future, versiones 2025–2026.

⁹ Análisis de curva de especificaciones sobre tres bases representativas de EE. UU. y Reino Unido, con 355.358 adolescentes. Encuentra una asociación negativa pequeña entre uso digital y bienestar: el uso digital explicaba como máximo cerca del 0,4 % de la variación. El estudio es robusto frente a selección de especificaciones, pero no identifica causalidad y depende de medidas autoinformadas. Orben, A., & Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3, 173–182. <https://doi.org/10.1038/s41562-018-0506-1>, pp. 173, 175 y 178–179.

la conclusión del estudio pueda extenderse automáticamente a los efectos de una plataforma, contenido o funcionalidad particular.

Otros análisis han encontrado efectos adversos en contextos específicos. Braghieri, Levy y Makarin aprovecharon la expansión gradual de Facebook en universidades estadounidenses para comparar la evolución de la salud mental entre instituciones que recibieron acceso a la plataforma en momentos diferentes. Encontraron un deterioro en indicadores de salud mental después de su introducción y mayores afectaciones académicas asociadas con problemas de salud mental¹⁰. Se trata de evidencia cuasiexperimental más apta para aproximarse a una relación causal, aunque corresponde a estudiantes universitarios y a una versión temprana de Facebook.

La evidencia agregada conduce a una conclusión igualmente matizada. Una revisión de 25 estudios encontró que la mayoría caracterizaba la relación entre redes sociales y salud mental adolescente como débil o inconsistente, mientras otras identificaban asociaciones más sustanciales y perjudiciales¹¹.

Un metaanálisis publicado en *JAMA Pediatrics* en 2024 abarcó 143 estudios que abordaron a más de un millón de adolescentes. Encontró asociaciones positivas, pero de magnitud pequeña, entre uso de redes sociales y síntomas internalizantes, acompañadas de diferencias muy grandes entre los estudios incluidos¹². El tamaño y amplitud de esta evidencia permiten sostener con mayor confianza la existencia de una asociación promedio; su elevada heterogeneidad impide asumir que esa asociación describe de igual manera a todos los adolescentes o todas las formas de uso.

La edad constituye una de esas fuentes potenciales de heterogeneidad. En un análisis longitudinal de 17.409 participantes, Orben et. al. encontraron periodos durante la adolescencia en los que un aumento del uso estimado de redes sociales se asociaba con reducciones posteriores en satisfacción con la vida, con diferencias según edad y sexo. También encontraron relaciones en la dirección inversa: una menor satisfacción podía preceder aumentos posteriores en el uso¹³. Los

¹⁰ Experimento natural sobre la introducción escalonada de Facebook en universidades de EE. UU., con diferencias en diferencias y cerca de 360.000 observaciones. La introducción de Facebook aumentó en 0,085 desviaciones estándar un índice de deterioro de salud mental, especialmente en depresión y ansiedad. La identificación es fuerte, pero el contexto corresponde a universitarios y a la expansión inicial de Facebook en 2004-2006. Braghieri, L., Levy, R., & Makarin, A. (2022). Social media and mental health. *American Economic Review*, 112(11), 3660–3693. <https://doi.org/10.1257/aer.20211218>, pp. 3663–3675.

¹¹ Revisión de 25 estudios sobre redes sociales y salud mental adolescente. Concluye que la mayoría de análisis encuentra asociaciones débiles o inconsistentes, aunque una minoría reporta efectos perjudiciales más sustanciales. Sirve para mostrar que la evidencia es heterogénea y depende del diseño, la medición y la población estudiada. Valkenburg, P. M., Meier, A., & Beyens, I. (2022). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. *Current Opinion in Psychology*, 44, 58–68. <https://doi.org/10.1016/j.copsyc.2021.08.017>.

¹² Metaanálisis de 143 estudios, 1.094.890 adolescentes y 886 tamaños de efecto. Encuentra asociaciones promedio pequeñas entre uso de redes y síntomas internalizantes, alrededor de $r=0,12$ a $r=0,14$, con heterogeneidad muy alta. La magnitud promedio es informativa, pero la mayoría de la evidencia sigue siendo observacional y autoinformada. Fassi, L., Thomas, K., Parry, D. A., Leyland-Craggs, A., Ford, T. J., & Orben, A. (2024). Social media use and internalizing symptoms in clinical and community adolescent samples: A systematic review and meta-analysis. *JAMA Pediatrics*, 178(8), 814–822. <https://doi.org/10.1001/jamapediatrics.2024.2078>.

¹³ Combina análisis transversales y longitudinales sobre 84.011 personas con un panel longitudinal de 17.409 participantes entre 10 y 21 años y 52.556 observaciones. Para el componente longitudinal utiliza Random-Intercept Cross-Lagged Panel Models, que separan diferencias estables entre personas de cambios dentro de cada individuo, modelos con máxima

resultados respaldan la importancia de considerar el desarrollo del adolescente, pero no permiten convertir esas edades directamente en umbrales regulatorios.

La investigación reciente también ha comenzado a mirar más allá del tiempo de uso. Un *Registered Report* con una muestra representativa de adolescentes británicos y evaluaciones diagnósticas realizadas por profesionales encontró que los adolescentes con determinadas condiciones de salud mental presentaban diferencias no solo en el tiempo dedicado a redes, sino también en comparación social, impacto emocional del *feedback* y satisfacción con sus relaciones en línea¹⁴.

Considerada conjuntamente, esta literatura permite sostener la existencia de riesgos relevantes, pero no un efecto único y uniforme del «uso de redes sociales». Edad, vulnerabilidad previa, contenido, modalidad de interacción, funcionalidades y contexto pueden modificar los resultados. La discusión científica no se encuentra cerrada respecto de la magnitud de esos efectos ni de los mecanismos que los producen. Por supuesto, esto no equivale a ausencia de riesgo.

1.3.2. Intervenciones, comportamiento y aprendizaje

Una segunda inquietud surge al pasar de la asociación al efecto de la intervención. No basta con preguntar si existe relación entre redes sociales, dispositivos digitales y bienestar; también es necesario examinar qué ocurre cuando una medida pública modifica efectivamente la forma, la intensidad o el contexto en que las personas usan esas tecnologías. Esa pregunta es central para valorar si una restricción general produce los efectos esperados, si genera sustituciones hacia otros usos digitales o si sus resultados dependen de la edad, el entorno y el tipo de acompañamiento previsto.

Un metaanálisis de 32 experimentos aleatorizados, con 5.544 participantes, encontró que restringir o suspender temporalmente el uso de redes sociales producía, en promedio, una mejora pequeña en bienestar. Sin embargo, los resultados variaban entre estudios y las muestras estaban conformadas por universitarios y adultos, no por niños o adolescentes de la población general¹⁵. Esta evidencia aporta una señal causal sobre la posibilidad de modificar el bienestar mediante

verosimilitud robusta, comparación de especificaciones y 500 réplicas bootstrap para representar incertidumbre. Identifica ventanas de sensibilidad en las que aumentos en el uso habitual de redes se asocian con menor satisfacción vital posterior, con diferencias por edad y sexo. Es relevante para la heterogeneidad del riesgo, aunque sigue siendo evidencia observacional. Orben, A., Przybylski, A. K., Blakemore, S.-J., & Kievit, R. A. (2022). Windows of developmental sensitivity to social media. *Nature Communications*, 13, Article 1649. <https://doi.org/10.1038/s41467-022-29296-3>.

¹⁴ Registered Report con 3.340 adolescentes del Reino Unido entre 11 y 19 años, con diagnósticos profesionales de salud mental. Los adolescentes con condiciones internalizantes reportaron más tiempo de uso, mayor comparación social y mayor impacto emocional del *feedback* en línea. El diseño mejora la medición, pero no permite establecer relaciones causales. Fassi, L., Ferguson, A. M., Przybylski, A. K., Ford, T. J., & Orben, A. (2025). Social media use in adolescents with and without mental health conditions. *Nature Human Behaviour*, 9, 1283–1299. <https://doi.org/10.1038/s41562-025-02134-4>.

¹⁵ Metaanálisis de 32 ensayos aleatorizados sobre reducción o suspensión de redes sociales, con 5.544 participantes. Encuentra una mejora promedio pequeña en bienestar subjetivo ($g=0,17$; IC 95 % 0,08–0,27). Es evidencia causal relevante sobre restricciones de uso, pero su validez externa para una prohibición general a menores es limitada, pues las muestras no corresponden a población infantil o adolescente comunitaria. Burnell, K., Meter, D. J., Andrade, F. C., Slocum, A. N., & George, M. J. (2025). The effects of social media restriction: Meta-analytic evidence from randomized controlled trials. *SSM – Mental Health*, 7, Article 100459. <https://doi.org/10.1016/j.ssmmh.2025.100459>.

restricciones de uso, pero todavía ofrece una base limitada para estimar el efecto de una prohibición general sobre menores.

Un experimento de Collis y Eggers ilustra además la posibilidad de sustitución. Los estudiantes asignados aleatoriamente al tratamiento redujeron el uso de Facebook, Instagram y Snapchat, pero trasladaron parte de ese tiempo hacia servicios de mensajería y no redujeron el tiempo total dedicado a dispositivos digitales. El estudio tampoco encontró mejoras significativas en bienestar o desempeño académico¹⁶.

La evidencia educativa muestra con particular claridad la importancia del contexto. Beland y Murphy estudiaron aproximadamente 130.000 estudiantes de 91 escuelas inglesas y encontraron mejoras en desempeño académico después de la introducción de prohibiciones de teléfonos móviles, concentradas principalmente entre los estudiantes de menor rendimiento previo¹⁷. Otros estudios realizados en contextos diferentes no han encontrado los mismos efectos, por lo que estos resultados tampoco constituyen evidencia de que cualquier prohibición de dispositivos produzca necesariamente mejoras académicas.

Dos experimentos aleatorizados desarrollados posteriormente en aulas permiten refinar esa conclusión. Deng y colaboradores encontraron que permitir el uso libre y no guiado del smartphone reducía el aprendizaje frente a mantenerlo fuera del aula; sin embargo, cuando el profesor dirigía su utilización con fines pedagógicos, los resultados superaban los obtenidos bajo la prohibición¹⁸.

La evidencia educativa no demuestra, por tanto, que prohibir redes sociales fuera del aula produzca necesariamente mejores resultados académicos. Sí muestra algo relevante para la discusión legislativa, una misma tecnología puede producir resultados diferentes según el contexto, la finalidad y la manera en que se utiliza. Esto permite distinguir una intervención dirigida a una fuente identificable de distracción en un entorno específico de una restricción aplicable de manera general a usos y circunstancias diferentes.

¹⁶ Ensayo aleatorizado en estudiantes universitarios que limitó Facebook, Instagram y Snapchat a diez minutos diarios, con medición objetiva del comportamiento digital. La intervención redujo el uso de esas redes, pero hubo sustitución hacia mensajería instantánea y no se observaron efectos significativos sobre bienestar o desempeño. Es útil para advertir que las restricciones pueden generar desplazamientos hacia otros usos digitales. Collis, A., & Eggers, F. (2022). Effects of restricting social media usage on wellbeing and performance: A randomized control trial among students. PLOS ONE, 17(8), e0272416. <https://doi.org/10.1371/journal.pone.0272416>.

¹⁷ Evaluación de impacto utilizando el método de diferencias en diferencias sobre prohibiciones de celulares en 91 escuelas inglesas, con cerca de 130.000 estudiantes. Los puntajes aumentaron alrededor de 0,07 desviaciones estándar tras la prohibición, y cerca de 0,14 entre estudiantes de menor desempeño previo. Sugiere que ciertas medidas pueden tener efectos diferenciados, aunque la interpretación causal depende de los supuestos del diseño. Beland, L. P., & Murphy, R. (2016). Ill communication: Technology, distraction & student performance. Labour Economics, 41, 61–76. <https://doi.org/10.1016/j.labeco.2016.04.004>, pp. 66–72.

¹⁸ Dos ensayos aleatorizados en una escuela vocacional china compararon prohibición, uso libre y uso pedagógicamente guiado de smartphones. El uso libre redujo la ganancia de aprendizaje, mientras el uso guiado la aumentó. El resultado es importante porque muestra que el problema no es solo acceso o no acceso, sino diseño del uso, contexto y supervisión. Deng, Z., Cheng, Z. A., Ferreira, P., & Pavlou, P. A. (2026). From smartphones to smart students: Learning vs. distraction using smartphones in the classroom. Information Systems Research, 37(1), 276–293. <https://doi.org/10.1287/isre.2022.0078>.

1.3.3. Australia y la evaluación de una restricción general por edad

Australia ofrece un punto de comparación especialmente útil porque permite observar los primeros resultados de una intervención nacional ya implementada. Desde el 10 de diciembre de 2025, las plataformas comprendidas por el régimen de edad mínima deben adoptar medidas razonables para evitar que menores de 16 años creen o mantengan cuentas. La evidencia inicial muestra una reducción en la tenencia de cuentas, pero un cambio mucho menor en el uso efectivo de las plataformas. Esto no permite concluir todavía sobre los efectos de largo plazo de la medida, pero sí muestra que su eficacia depende críticamente de la implementación técnica, de la capacidad real de las plataformas para aplicar mecanismos de garantía de edad y de evitar que la restricción se traduzca solo en acceso sin cuenta, subdeclaración de edad o desplazamiento hacia otros servicios¹⁹.

La evaluación desarrollada por eSafety, en colaboración con el Social Media Lab de Stanford y un grupo académico asesor independiente, sigue durante más de dos años a más de 4.000 niños y a uno de sus padres o cuidadores²⁰. El propio diseño de la evaluación distingue entre las condiciones necesarias para implementar la política y los resultados finales que esta pretende producir: primero deben operar adecuadamente la garantía de edad y la reducción de cuentas; posteriormente podrían observarse cambios en utilización, exposición a riesgos y, eventualmente, bienestar.

El informe de seguimiento a tres meses recoge datos de línea base previos a la entrada en vigor de la medida y una medición posterior en niños de 10 a 15 años. Reporta una caída en la tenencia de cuentas en plataformas restringidas de 52,4% a 42,1%, mientras el uso efectivo de al menos una plataforma restringida disminuyó de 85,9% a 81,5%. La frecuencia de uso cambió poco, alrededor de tres de cada cinco niños reportaban usar redes sociales al menos diariamente en ambos momentos.

La distancia entre tenencia de cuenta y utilización es particularmente relevante. Los menores pueden acceder a determinados contenidos sin una cuenta propia, utilizar cuentas compartidas o mantener cuentas que todavía no han sido sometidas a una comprobación efectiva. Aproximadamente la mitad de quienes conservaron cuentas manifestó que la plataforma no había comprobado todavía su edad. Otros aparecían registrados como mayores de 16 años o habían sido clasificados incorrectamente por el mecanismo utilizado.

¹⁹ Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. (2026). Current legislation: Social media minimum age. Australian Government. <https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation>; Office of the Australian Information Commissioner. (2025). Social Media Minimum Age. Australian Government. <https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-minimum-age>; eSafety Commissioner. (2026). Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow-up. Australian Government, pp. 6-11, 22-25 y 36-37. <https://www.esafety.gov.au/sites/default/files/2026-08/Early-days-Early-Insights-SMMA-Evaluation-Understanding-experiences-of-social-media-age-restrictions-August2026.pdf>

²⁰ AUSTRALIA. eSafety Commissioner. *Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow-up*. Julio de 2026. <https://www.esafety.gov.au/research/social-media-age-restrictions-evaluation/early-days-early-insights-three-months-report>

La utilización de mecanismos deliberados de evasión —como documentos de terceros, VPN o nuevas cuentas después de una desactivación— fue comparativamente reducida. En esta primera medición, eSafety identifica la implementación todavía incompleta de los mecanismos de garantía de edad como la principal explicación de la permanencia de cuentas²¹.

La evaluación registra también señales que requieren seguimiento. Entre los menores que continuaban utilizando redes sociales, la proporción de padres que desconocía ese uso pasó aproximadamente de uno de cada cuatro a uno de cada tres. También aumentaron el uso de servicios de mensajería y la frecuencia de videojuegos en línea. eSafety presenta estos movimientos como posibles señales de redistribución de actividades y advierte que todavía no puede determinar si son causados por la restricción ni si persistirán en el tiempo.

En otros resultados —participación en actividades fuera de línea y comportamientos asociados con uso problemático, como dejar de comer o dormir— la evaluación encontró pocos cambios a los tres meses. Cerca de dos terceras partes de los niños reportaron, además, que la medida no había tenido todavía impacto en sus vidas.

Las conclusiones preliminares permiten diferenciar tres niveles. La reducción de cuentas informa sobre implementación; los cambios en utilización y la posible migración hacia otros servicios informan sobre comportamiento; la reducción de exposición a riesgos, daños o afectaciones al bienestar corresponde al resultado final que justifica la intervención. Australia ya ofrece evidencia sobre los dos primeros niveles, pero su propia autoridad señala que todavía es demasiado temprano para evaluar de manera significativa si se alcanzarán los resultados de largo plazo.

Esta distinción resulta particularmente importante para la deliberación legislativa. La evidencia científica puede sustentar la existencia de determinados riesgos y la experiencia australiana muestra que una restricción puede reducir la tenencia formal de cuentas. Establecer en qué medida esa reducción se traduce en una disminución suficiente y sostenida del daño constituye una pregunta empírica diferente, cuya respuesta todavía se encuentra en construcción.

1.4. Garantías frente a medidas de mayor intensidad en el derecho comparado

La experiencia comparada muestra que las restricciones de edad en entornos digitales están creciendo, pero no existe un modelo único ni evidencia concluyente de que una prohibición general produzca, por sí sola, mejores resultados de protección. La OCDE ha identificado un aumento de iniciativas sobre restricciones de edad para redes sociales y servicios digitales, aunque con diseños muy distintos: algunos ordenamientos establecen edades mínimas para mantener cuentas; otros imponen autorización parental, deberes reforzados de diseño seguro o medidas de garantía de edad diferenciadas según el tipo de servicio y riesgo²².

²¹ eSafety Commissioner. (2026). Early days, early insights: Understanding experiences of social media age restrictions at the three-month follow-up. Australian Government.

²² OCDE. (2026, 14 de abril). Social media age restrictions for children: Why they are rising and what comes next. <https://www.oecd.org/en/blogs/2026/04/social-media-age-restrictions-for-children-why-they-are-rising-and-what-comes-next.html>; OCDE. (2025). Age assurance practices of 50 online services used by children. OECD Publishing. <https://doi.org/10.1787/a19853ab-en>

En Estados Unidos, una parte relevante del debate reciente no se ha concentrado únicamente en la edad mínima, sino en los defectos de diseño atribuidos a las plataformas²³. Las demandas de fiscales generales contra Meta, así como litigios sobre redes sociales y salud mental, han puesto el foco en funcionalidades como desplazamiento infinito, reproducción automática, notificaciones persistentes, métricas de aprobación social, recomendaciones algorítmicas y otros mecanismos de maximización de permanencia.

Al mismo tiempo, la jurisprudencia constitucional de los Estados Unidos²⁴ muestra que las medidas dirigidas a proteger menores deben diferenciar cuidadosamente entre tipos de contenidos, servicios y mecanismos regulatorios. En *Brown v. Entertainment Merchants Association*, la Corte Suprema invalidó una restricción al acceso de menores a videojuegos violentos, al considerar que el Estado no podía crear nuevas categorías de expresión no protegida ni sustituir, de manera general, la decisión parental. En contraste, en *Free Speech Coalition, Inc. v. Paxton*, la Corte admitió la exigencia de verificación de edad para sitios con contenidos sexuales nocivos para menores, al tratarse de un ámbito tradicionalmente sujeto a mayores restricciones frente al acceso infantil. Estos antecedentes son útiles porque desplazan la pregunta desde «qué edad debe tener el usuario» hacia una más precisa: qué tipo de contenido, funcionalidad o diseño genera el riesgo; qué nivel de restricción resulta proporcional; y qué garantías deben acompañar los mecanismos de verificación o limitación de acceso.

El caso francés ofrece un antecedente especialmente útil sobre los límites constitucionales de las prohibiciones generales. En 2026, el Consejo Constitucional examinó una ley dirigida a proteger a los menores frente a riesgos asociados al uso de redes sociales. La norma incluía, entre otros componentes, una prohibición de acceso para menores de 15 años. El Consejo consideró problemático que la medida operara de manera general sobre servicios diversos, sin distinguir suficientemente entre funcionalidades, niveles de riesgo, medidas de protección existentes ni márgenes de decisión parental. También advirtió que una restricción de esa naturaleza podía afectar la libertad de expresión y comunicación, así como el respeto de la vida privada, en la medida en que la comprobación de edad podía terminar exigiéndose a todos los usuarios, incluidos los adultos²⁵.

Ese antecedente se conecta con las advertencias de la CNIL francesa sobre verificación de edad. Para esta autoridad, los sistemas de comprobación de edad pueden resultar intrusivos o fáciles de eludir si no se diseñan bajo criterios de minimización, proporcionalidad, robustez y separación entre verificación de edad e identificación de la persona²⁶. Así, no es que toda garantía de edad sea

²³ National Association of Attorneys General. (2023). *Attorneys general sue Meta over harmful features for youth*. <https://www.naag.org/>; In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, MDL No. 3047; Estado de Nuevo México v. Meta Platforms, Inc.; Estado de Alabama v. TikTok Inc.

²⁴ *Brown v. Entertainment Merchants Association*, 564 U.S. 786, 799–805 (2011); *Free Speech Coalition, Inc. v. Paxton*, No. 23-1122, slip op. at 5–36 (U.S. Supreme Court, June 27, 2025)

²⁵ Conseil constitutionnel. (2026, 14 de agosto). *Décision n° 2026-911 DC, Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*. <https://www.conseil-constitutionnel.fr/decision/2026/2026911DC.htm>

²⁶ Commission Nationale de l'Informatique et des Libertés. (2022, 26 de julio). *Vérification de l'âge en ligne: Trouver l'équilibre entre protection des mineurs et respect de la vie privée*. <https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>

inadmisible, sino que debe definirse con precisión qué dato se exige, quién lo trata, por cuánto tiempo, con qué finalidad, bajo qué controles y con qué alternativas menos intrusivas.

En la Unión Europea, el Reglamento de Servicios Digitales ofrece una aproximación distinta a la prohibición general. Su artículo 28 exige que las plataformas accesibles a menores adopten medidas apropiadas y proporcionadas para garantizar un alto nivel de privacidad, seguridad y protección. Las directrices europeas sobre esta disposición y la Recomendación (UE) 2026/1035 sobre verificación de edad desarrollan un estándar técnico relevante: la comprobación de edad debe ser precisa, fiable, robusta, discreta, no discriminatoria y respetuosa de la protección de datos. En particular, debe evitar revelar identidad, fecha exacta de nacimiento, ubicación, patrones de navegación o información que permita seguimiento entre servicios, cuando baste con acreditar que la persona supera un umbral de edad²⁷.

Ese mismo enfoque ha sido reforzado por el Comité Europeo de Protección de Datos y la Agencia Española de Protección de Datos²⁸. Ambos admiten que, en ciertos contextos, puede ser necesario establecer si un usuario supera determinada edad; sin embargo, exigen que el método sea idóneo, necesario, proporcionado y minimice datos. En términos prácticos, esto implica preferir soluciones que acrediten un resultado binario —por ejemplo, supera/no supera determinada edad— sin convertir la garantía de edad en un mecanismo generalizado de identificación, trazabilidad o perfilamiento.

Japón aporta un argumento complementario desde la protección de datos biométricos²⁹. La reforma de 2026 a su Ley de Protección de la Información Personal no constituye una prohibición general de la biometría ni una regla específica sobre redes sociales; sin embargo, sí resulta pertinente para este debate porque refuerza las salvaguardas aplicables a información biométrica capaz de identificar o seguir a una persona, especialmente cuando puede captarse sin que esta lo advierta fácilmente. Este antecedente muestra que, si la comprobación de edad se apoya en reconocimiento facial u otros rasgos biométricos, el legislador debe prever garantías reforzadas de transparencia, finalidad, derechos de oposición o supresión, límites a transferencias y controles frente a seguimiento o perfilamiento.

UNICEF advierte que las restricciones basadas exclusivamente en edad pueden generar efectos no deseados. Entre ellos se encuentran el desplazamiento de niños, niñas y adolescentes hacia

²⁷ Comisión Europea. (2025, 10 de octubre). *Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065*. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52025XC05519>; Comisión Europea. (2026, 29 de abril). *Recomendación (UE) 2026/1035 sobre el establecimiento de un marco común para las tecnologías de verificación de la edad a escala de la Unión Europea*. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-80678>

²⁸ Comité Europeo de Protección de Datos. (2025, 11 de febrero). *Statement 1/2025 on age assurance*. https://www.edpb.europa.eu/documents/statement/statement-12025-on-age-assurance_en; Agencia Española de Protección de Datos. (2023). *Decálogo de principios: Verificación de edad y protección de menores de edad ante contenidos inadecuados*. <https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf>

²⁹ Japón, Cámara de Representantes. (2026). *Bill for partial amendment of the Act on the Protection of Personal Information and related laws*, Cabinet Bill No. 54, 221st Diet. https://www.shugiin.go.jp/Internet/itdb_gian.nsf/html/gian/honbun/houan/q22109054.htm

servicios menos regulados, la restricción de acceso a información educativa, de salud o apoyo comunitario, impactos diferenciados sobre poblaciones en situación de vulnerabilidad, riesgos para la privacidad derivados de la verificación de edad y una posible reducción de incentivos para que las plataformas adopten diseños más seguros. Por ello, UNICEF recomienda que estas medidas se acompañen de evaluaciones de impacto en derechos de la niñez, definición precisa de los daños que se buscan prevenir, delimitación clara de servicios y funcionalidades cubiertas, y sistemas de monitoreo sobre resultados reales³⁰.

En suma, la experiencia comparada ofrece criterios útiles para el análisis legislativo, pero también muestra que las medidas de mayor intensidad requieren una calibración detallada. Cuando una regulación limita el acceso de niños, niñas y adolescentes a determinados servicios digitales, resulta necesario precisar su finalidad, justificar su necesidad, diferenciar los niveles de riesgo, proteger los datos personales, prever mecanismos de reclamación y evaluar sus efectos reales. Así, la pregunta central no es solo cuál debe ser la edad mínima, sino qué riesgos concretos se buscan prevenir, qué funcionalidades justifican medidas más estrictas, qué información puede tratarse para verificar la edad y qué garantías deben existir frente a errores, evasión, exclusión o desplazamiento hacia entornos menos seguros.

1.5. Riesgos regulatorios y técnicos derivados de las experiencias internacionales

Las experiencias internacionales revisadas permiten identificar algunos riesgos que conviene considerar al diseñar medidas de protección de niños, niñas y adolescentes en entornos digitales. Estos riesgos no desvirtúan la finalidad protectora de la intervención legislativa; por el contrario, ayudan a precisar sus condiciones de eficacia, proporcionalidad e implementación.

1. **Rigidez regulatoria y rápida obsolescencia.** Una prohibición definida únicamente a partir de la categoría de «red social» o de una lista cerrada de servicios definida a nivel legal puede quedar rápidamente desactualizada frente a la convergencia entre redes sociales, mensajería, videojuegos, plataformas de video, transmisiones en vivo, tiendas de aplicaciones, comunidades digitales y servicios de inteligencia artificial conversacional. Esto puede producir dos efectos, por un lado, tratar de manera distinta funcionalidades semejantes y, por otro lado, dejar por fuera servicios que, aunque no se presenten como redes sociales, incorporan interacción entre usuarios, recomendación algorítmica, exposición pública, monetización o contacto con desconocidos.
2. **Riesgo de desalineación entre el tipo de contenido, la funcionalidad y la intensidad de la medida.** La experiencia comparada muestra que no todas las restricciones de acceso tienen el mismo fundamento ni enfrentan el mismo estándar de justificación. En Estados Unidos, por ejemplo, la Corte Suprema invalidó en *Brown v. Entertainment Merchants Association* una restricción al acceso de menores a videojuegos

³⁰ UNICEF. (2025). *Trazando una línea en los espacios digitales: Restricción del uso de las redes sociales según la edad*. https://www.unicef.org/media/176716/file/UNICEF%20policy%20note_age%20restrictions%20social%20media_SPANISH.pdf.pdf

violentos, mientras que en Free Speech Coalition, Inc. v. Paxton admitió una exigencia de verificación de edad para sitios con contenidos sexuales nocivos para menores. La utilidad de estos precedentes no está en trasladar mecánicamente sus soluciones, sino en advertir que el análisis debe diferenciar entre tipos de contenido, servicios, funcionalidades, riesgos y mecanismos de verificación.

3. **Desplazamiento de la protección integral hacia una barrera de acceso.** Las restricciones de edad pueden ser una herramienta relevante, pero no sustituyen las obligaciones de seguridad que deben aplicarse al diseño y operación de los servicios. Si la medida se concentra solo en impedir la creación o mantenimiento de cuentas, puede dejar sin intervención factores que producen o amplifican riesgos: sistemas de recomendación, contacto no solicitado con adultos desconocidos, publicidad dirigida, perfilamiento, geolocalización, transmisiones en vivo, moderación deficiente, compras integradas, reproducción automática, desplazamiento infinito, notificaciones persistentes o recompensas variables. La pregunta regulatoria no es solo quién puede acceder, sino bajo qué condiciones funciona el servicio cuando es accesible para adolescentes.
4. **Impactos diferenciados sobre determinados grupos de niños y adolescentes.** Una medida general puede cubrir servicios de bajo riesgo, como herramientas educativas, comunidades cerradas o espacios de apoyo, y al mismo tiempo dejar por fuera funcionalidades de alto riesgo presentes en otros entornos digitales. Además, las restricciones pueden afectar de manera distinta a adolescentes que utilizan estos servicios para acceder a información educativa, recursos de salud, comunidades de apoyo, participación social o expresión cultural. UNICEF ha advertido que las restricciones basadas exclusivamente en edad pueden generar desplazamiento hacia servicios menos regulados, limitar el acceso a recursos beneficiosos, producir efectos más intensos sobre quienes cuentan con menos alternativas presenciales y generar condiciones inequitativas sobre aquellos que cuentan con menores recursos económicos.
5. **Clasificación, garantías del debido proceso y protección de datos personales de los usuarios.** Los sistemas de garantía de edad plantean un riesgo específico de confiabilidad y proporcionalidad. Por un lado, pueden generar errores de clasificación como son: menores que evaden la restricción, adolescentes habilitados que son bloqueados indebidamente o adultos que deben acreditar su edad para acceder a servicios lícitos. Por otro lado, la forma de corregir esos errores no puede consistir en exigir, por defecto, más datos de los necesarios. Algunos métodos pueden involucrar información sensible o altamente identificable, como documentos de identidad, fecha exacta de nacimiento, reconocimiento facial, datos biométricos o señales que permitan seguimiento entre servicios. Por ello, la experiencia europea apunta a una regla técnica central: **acreditar edad no debe confundirse con identificar plenamente a la persona**. Cuando baste con establecer si un usuario supera determinado umbral, el sistema debería limitarse a entregar ese resultado, sin revelar información adicional ni permitir su reutilización para publicidad, perfilamiento o trazabilidad. Esta misma lógica exige prever mecanismos claros de reclamación, corrección y restitución rápida de cuentas, de manera que la protección

de menores no produzca restricciones injustificadas sobre adolescentes habilitados o adultos, y al mismo tiempo mejore la efectividad frente a intentos reales de evasión.

6. **Medición incompleta de la eficacia.** La reducción en el número de cuentas creadas, bloqueadas o eliminadas no permite concluir, por sí sola, que disminuyeron los riesgos para niños, niñas y adolescentes. Puede existir una caída en la tenencia formal de cuentas, pero mantenerse el uso efectivo mediante cuentas de terceros, evasión, migración hacia servicios no cubiertos o desplazamiento hacia espacios menos regulados. Por ello, las evaluaciones deberían considerar indicadores sobre uso real, mecanismos de evasión, incidentes de daño, errores de clasificación, reclamaciones, restitución de cuentas, afectaciones a la privacidad y acceso a recursos beneficiosos.

En conjunto, estos riesgos sugieren que la protección efectiva de niños, niñas y adolescentes requiere combinar reglas de acceso, obligaciones de diseño seguro, garantía de edad proporcional al riesgo, minimización de datos, procedimientos de reclamación y evaluación periódica. La edad puede ser un criterio relevante, pero su eficacia depende de cómo se integre con medidas dirigidas a los riesgos concretos que surgen de las funcionalidades, los modelos de negocio y las formas reales de uso de los servicios digitales.

1.6. Marco normativo y constitucional colombiano aplicable

El análisis del Proyecto de Ley puede apoyarse en un marco colombiano reciente que ya reconoce la necesidad de proteger a niños, niñas y adolescentes en entornos digitales, sin reducir esa protección a una única herramienta regulatoria. La Ley 2489 de 2025³¹ estableció disposiciones para promover entornos digitales sanos y seguros, a partir de la articulación entre Estado, familias, sector privado, organizaciones sociales y sociedad en general. Su objeto, expresado en el artículo 1, combina prevención y educación de riesgos en línea, promoción de hábitos saludables en el uso de tecnología y garantía de derechos.

Dicha ley incorpora principios relevantes para el trámite legislativo. Tales principios son, de acuerdo con el artículo 3, los de corresponsabilidad; interés superior de niños, niñas y adolescentes; protección integral del menor; evolución de las facultades de los niños, niñas y adolescentes; proporcionalidad; enfoque basado en el respeto a los derechos humanos. En lo que concierne al principio de proporcionalidad, el citado artículo 3 dispone, entre otras cosas, que las medidas de protección deben ser proporcionales a los riesgos, basadas en evidencia, efectivas y equilibradas; promover la libertad de expresión de niños, niñas y adolescentes; no socavar otros derechos humanos; y no restringir indebidamente la provisión de servicios digitales ni la innovación que pueda favorecer un entorno digital seguro y beneficioso.

La Ley 2489 también reconoce expresamente que niños, niñas y adolescentes tienen derecho a buscar, recibir y difundir informaciones e ideas por medio de entornos digitales seguros, con el

³¹ Congreso de la República de Colombia. (2025). Ley 2489 de 2025, por medio de la cual se establecen disposiciones para el desarrollo de entornos digitales sanos y seguros para los niños, niñas y adolescentes del país. Diario Oficial No. 53.185, 18 de julio de 2025. Disponible en: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=185913>

acompañamiento correspondiente de padres, cuidadores o tutores. Al mismo tiempo, admite restricciones orientadas a proteger su bienestar, desarrollo e integridad, así como la seguridad y los derechos de otras personas. Esta combinación es importante para el análisis del proyecto, pues el ordenamiento colombiano ya parte de una lógica de protección reforzada, pero también de acceso, participación, autonomía progresiva y garantías.

En este sentido, el Decreto 769 de 2026³² desarrolla esa orientación mediante un enfoque basado en riesgos. Para ello, prevé que las medidas se apliquen de manera diferenciada según la naturaleza del servicio, el nivel de riesgo, el grado de interacción con niños, niñas y adolescentes, la capacidad técnica y operativa de los actores y las competencias legales de las autoridades involucradas. También señala que no deben imponerse cargas automáticas o uniformes a todos los actores del ecosistema digital, y que las medidas no pueden implicar censura previa, monitoreo generalizado de contenidos ni restricciones injustificadas al acceso a la información o a los servicios digitales.

En materia de garantía de edad, el Decreto 769 ofrece un criterio técnico especialmente relevante. Los mecanismos de verificación deben ser acordes con el nivel de riesgo, aplicar estrictamente el principio de minimización de datos y cumplir el régimen de protección de datos personales. Además, el decreto excluye medidas que impliquen monitoreo masivo o indiscriminado de comunicaciones, debilitamiento del cifrado, bloqueo generalizado de plataformas, recolección de datos biométricos, perfilamiento algorítmico comercial de niños, niñas y adolescentes o vigilancia masiva sin orden judicial. Esto permite distinguir entre acreditar un umbral de edad y construir sistemas generales de identificación o trazabilidad de usuarios.

La jurisprudencia constitucional ofrece criterios adicionales para valorar este tipo de medidas. La Corte Constitucional ha sostenido que la libertad de expresión tiene una presunción de protección reforzada, que las limitaciones estatales sobre ella son constitucionalmente sospechosas y que la censura previa está prohibida. También ha señalado que existen categorías de expresión no protegidas, como la pornografía infantil, la incitación directa y pública al genocidio, la propaganda de guerra y la apología del odio que constituya incitación a la discriminación, hostilidad o violencia. Fuera de esos supuestos, las restricciones deben ser precisas, necesarias y proporcionadas³³.

En relación con redes sociales e internet, la Corte ha reconocido que estos espacios cumplen una función relevante para la circulación de ideas, información, participación pública y ejercicio de otros derechos. En la Sentencia SU-420 de 2019³⁴, la Corte indicó que lo publicado en redes sociales está amparado por la libertad de expresión, aunque sujeto a límites cuando se afecten derechos de

³² Presidencia de la República de Colombia. (2026). *Decreto 769 de 2026, por el cual se adiciona un título al Decreto 1078 de 2015*. Diario Oficial No. 53.556, 17 de julio de 2026. Disponible en: https://normograma.com/crc/compilacion/docs/decreto_0769_2026.htm

³³ Corte Constitucional de Colombia. (2007). *Sentencia T-391 de 2007*. M.P. Manuel José Cepeda Espinosa. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2007/T-391-07.htm>; Corte Constitucional de Colombia. (2011). *Sentencia C-442 de 2011*. M.P. Humberto Antonio Sierra Porto. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2011/C-442-11.htm>

³⁴ Corte Constitucional de Colombia. (2019). *Sentencia SU-420 de 2019*. M.P. José Fernando Reyes Cuartas. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm>

terceros. También señaló que el análisis debe considerar quién comunica, sobre quién se comunica, cuál es el contenido, cuál es el canal utilizado y cuál es el impacto de la publicación.

Más recientemente, la Sentencia T-256 de 2025³⁵ desarrolló reglas sobre moderación de contenidos en plataformas digitales. La Corte reconoció que las plataformas pueden adoptar normas comunitarias, pero precisó que esas reglas deben respetar derechos fundamentales. En particular, destacó la importancia de la transparencia, la aplicación consistente y no discriminatoria de las reglas, la explicación de las decisiones, los mecanismos de reclamación y la proporcionalidad de las sanciones cuando se restringen contenidos o cuentas.

La Corte también ha protegido el acceso a información en canales digitales. En la Sentencia T-475 de 2024³⁶, al estudiar el bloqueo de un periodista por parte de una cuenta oficial en X, señaló que las redes utilizadas por autoridades públicas pueden constituir espacios relevantes de comunicación e interacción sobre asuntos de interés general. Por ello, una restricción injustificada puede afectar tanto el acceso a información pública como la libertad de expresión y de prensa. A su vez, en la Sentencia T-372 de 2023³⁷, la Corte resaltó que internet no puede entenderse únicamente como un servicio público, pues permite informarse, adquirir conocimiento, tomar decisiones e interactuar en comunidad.

En materia de datos personales, la Corte Constitucional ha sostenido que el tratamiento de datos de niños, niñas y adolescentes exige una protección reforzada. La Sentencia C-748 de 2011³⁸ indicó que dicho tratamiento debe asegurar el respeto prevalente de sus derechos y estar acompañado de educación sobre los riesgos del uso indebido de datos personales. La Sentencia C-468 de 2025³⁹ reiteró que el tratamiento no está absolutamente prohibido, pero debe responder al interés superior, asegurar el respeto de los derechos fundamentales y, cuando involucre información sensible, imagen, intimidad o habeas data de niños, niñas y adolescentes, superar un juicio estricto de proporcionalidad.

A partir de este marco, el Proyecto de Ley puede leerse como una oportunidad para complementar y precisar la política pública vigente. Para ello, conviene valorar si sus medidas se articulan con la Ley 2489 de 2025 y el Decreto 769 de 2026, si distinguen entre servicios y funcionalidades, si se apoyan en un enfoque basado en riesgos, si prevén garantías de minimización de datos y si incorporan mecanismos de reclamación y corrección frente a posibles errores de clasificación o restricción de cuentas.

³⁵ Corte Constitucional de Colombia. (2025). *Sentencia T-256 de 2025*. M.P. Natalia Ángel Cabo. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2025/t-256-25.htm>

³⁶ Corte Constitucional de Colombia. (2024). *Sentencia T-475 de 2024*. M.P. Antonio José Lizarazo Ocampo. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2024/T-475-24.htm>

³⁷ Corte Constitucional de Colombia. (2023). *Sentencia T-372 de 2023*. M.P. Natalia Ángel Cabo. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2023/T-372-23.htm>

³⁸ Corte Constitucional de Colombia. (2011). *Sentencia C-748 de 2011*. M.P. Jorge Ignacio Pretelt Chaljub. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2011/C-748-11.htm>

³⁹ Corte Constitucional de Colombia. (2025). *Sentencia C-468 de 2025*. Disponible en: <https://www.corteconstitucional.gov.co/relatoria/2025/C-468-25.htm>

En ese sentido, el marco colombiano no impide adoptar medidas adicionales de protección; de hecho, ofrece criterios para fortalecerlas: finalidad clara, proporcionalidad, diferenciación según riesgo, diseño seguro por defecto, protección de datos, respeto por la libertad de expresión y acceso a la información, debido proceso en decisiones que afecten cuentas o contenidos, y evaluación periódica de resultados. Estos elementos permiten avanzar hacia una regulación protectora, técnicamente aplicable y armónica con el ordenamiento vigente.

2. Comentarios técnicos al proyecto de ley

A partir de la revisión comparada y del marco colombiano vigente, los comentarios al Proyecto de Ley se presentan en dos niveles: primero, unos criterios generales para valorar la coherencia, proporcionalidad e implementación de la iniciativa; y segundo, observaciones específicas al articulado.

2.1. Comentarios generales

A partir de la revisión comparada y del marco colombiano vigente, esta sección identifica los criterios transversales para analizar el Proyecto de Ley antes de abordar el articulado. El punto de partida es que la protección de niños, niñas y adolescentes en entornos digitales no debería formularse como una elección binaria entre permitir o prohibir el acceso, sino como una regulación diferenciada según los riesgos que se buscan mitigar, las funcionalidades involucradas, las competencias institucionales, las garantías de edad, la protección de datos, el debido proceso y la evaluación de resultados.

En ese contexto, el análisis del Proyecto de Ley puede organizarse alrededor de los siguientes elementos:

1. **Armonización con el marco vigente.** Propender por la articulación del proyecto con la Ley 2489 de 2025 y el Decreto 769 de 2026. Más que crear un régimen paralelo, la iniciativa puede fortalecer el marco existente si precisa obligaciones, instrumentos de implementación, autoridades competentes, plazos, mecanismos de seguimiento y garantías para los usuarios. Esto es especialmente relevante porque el ordenamiento colombiano ya adoptó una aproximación basada en protección integral, proporcionalidad, evolución de facultades y enfoque de derechos, y porque el Decreto 769 de 2026 prevé desarrollos técnicos a cargo del Ministerio TIC, en coordinación con la CRC, para orientar a los distintos actores según su rol, capacidad de intervención y nivel de riesgo asociado al servicio o funcionalidad.
2. **Definición del riesgo que se busca mitigar.** La discusión no debería limitarse a la edad de acceso. Resulta útil identificar con mayor precisión cuáles riesgos justifican la intervención, como podrían ser: contacto no solicitado por adultos, exposición a contenido inapropiado, explotación sexual, ciberacoso, perfilamiento publicitario, uso compulsivo, compras integradas, recomendación algorítmica, transmisión en vivo, geolocalización o difusión pública de perfiles. Esta precisión permite evitar reglas excesivamente amplias y

facilita que las obligaciones recaigan sobre las funcionalidades que realmente generan o amplifican el riesgo.

3. **Delimitación del ámbito de aplicación.** Para una implementación clara, conviene distinguir entre tipos de servicios y funcionalidades. No presentan el mismo riesgo una red social abierta, una aplicación de mensajería familiar, una plataforma educativa, un videojuego con interacción entre desconocidos, una tienda de aplicaciones, una plataforma de video, un servicio de inteligencia artificial conversacional o un entorno de transmisión en vivo. El proyecto podría diferenciar entre acceso al servicio, creación o mantenimiento de cuentas, acceso a funcionalidades específicas y exposición a determinados contenidos.
4. **Garantía de edad proporcional al nivel de riesgo.** La garantía de edad puede ser una herramienta útil, pero su intensidad debería depender del riesgo del servicio o funcionalidad. La autodeclaración simple puede ser insuficiente para servicios de alto riesgo, mientras que la verificación documental o biométrica generalizada puede resultar excesiva para servicios de menor riesgo. El criterio técnico más consistente con la experiencia comparada y el marco colombiano es que el proveedor conozca solo lo estrictamente necesario para aplicar la medida, por ejemplo, si el usuario supera o no determinado umbral de edad, sin acceder a identidad completa, fecha exacta de nacimiento, documento, ubicación o datos biométricos, salvo que exista una justificación estricta y garantías reforzadas.
5. **Diseño seguro por defecto.** La protección no debería descansar únicamente en impedir o permitir el acceso. Una regulación más completa puede diseñarse para incorporar obligaciones sobre el diseño mismo del servicio: configuración protectora por defecto para usuarios menores de edad, límites a recomendaciones basadas en perfilamiento, restricciones a publicidad dirigida, controles frente a mensajes de adultos desconocidos, opciones proporcionadas de supervisión parental, rutas eficaces de denuncia, moderación adecuada y restricciones sobre mecanismos que incentiven uso compulsivo. Esta aproximación permite intervenir las condiciones que producen el riesgo, no solo la edad del usuario.
6. **Protección de datos y privacidad.** Todo sistema de garantía de edad implica algún grado de tratamiento de información. Por ello, el proyecto debería incorporar reglas claras sobre minimización de datos, finalidad, conservación, seguridad, prohibición de reutilización para publicidad o perfilamiento, transparencia frente al usuario y mecanismos de supresión o corrección. Este punto es especialmente sensible si se contemplan documentos de identidad, reconocimiento facial, estimaciones biométricas o herramientas que puedan permitir seguimiento entre servicios.
7. **Libertad de expresión, acceso a información y participación.** El marco constitucional colombiano reconoce que internet y las redes sociales son espacios relevantes para informarse, expresarse, participar e interactuar. Por ello, cualquier restricción debería cuidar que la protección de niños, niñas y adolescentes no produzca exclusiones innecesarias frente a recursos educativos, de salud, participación comunitaria,

apoyo emocional o información de interés público. La regulación puede distinguir mejor entre contenidos o funcionalidades de alto riesgo y espacios digitales que cumplen funciones legítimas para el desarrollo, la educación y la participación de adolescentes.

8. **Debido proceso y mecanismos de reclamación.** Los sistemas de restricción o verificación de edad pueden generar errores. Pueden bloquearse adolescentes habilitados, adultos, cuentas familiares o usuarios que no logran completar el proceso de verificación. El proyecto podría prever garantías mínimas: notificación clara, explicación de la decisión, mecanismo sencillo de reclamación, corrección de errores, revisión humana cuando corresponda, restitución rápida de cuentas y canales diferenciados para niños, niñas, adolescentes y responsables legales. Estas garantías no debilitan la medida; aumentan su legitimidad y reducen restricciones injustificadas.
9. **Gobernanza institucional y competencias.** La implementación requiere claridad sobre el rol de cada autoridad. El proyecto puede fortalecer la coordinación entre entidades sin generar duplicidad de funciones ni cargas operativas difíciles de ejecutar. También conviene diferenciar entre regulación técnica, pedagogía, protección de datos, protección del consumidor, restablecimiento de derechos, investigación penal y supervisión de obligaciones a plataformas o proveedores. Una arquitectura institucional clara facilita el cumplimiento y reduce incertidumbre para usuarios, familias, autoridades y agentes del ecosistema digital.
10. **Evaluación de impacto y revisión periódica.** La eficacia de la medida no debería medirse únicamente por el número de cuentas bloqueadas, eliminadas o restringidas. Sería útil establecer el diseño de indicadores sobre uso efectivo, desplazamiento hacia servicios no cubiertos, incidentes de daño, reclamaciones, falsos positivos y falsos negativos, afectaciones a la privacidad, tiempos de resolución, acceso a recursos educativos o de apoyo, y cambios verificables en funcionalidades de diseño. Además, una cláusula de revisión periódica permitiría ajustar la regulación frente a cambios tecnológicos en verificación de edad, evasión, recomendación algorítmica e interacción entre usuarios.

Considerando estos elementos, el Proyecto de Ley puede avanzar hacia un modelo de protección por niveles de riesgo. Los servicios o contenidos exclusivamente para adultos pueden justificar mecanismos más robustos de verificación. Las redes sociales y plataformas de interacción masiva pueden requerir garantía de edad, configuración protectora por defecto y límites a funcionalidades de alto riesgo. Los servicios educativos, de salud, apoyo, comunicación familiar o participación comunitaria pueden requerir un tratamiento diferenciado para evitar exclusiones injustificadas.

Esta aproximación permite construir una regulación más precisa que protege a niños, niñas y adolescentes frente a riesgos reales, preserva sus derechos en entornos digitales, reduce cargas innecesarias sobre servicios de bajo riesgo y facilita una implementación técnica verificable.

2.2. Comentarios específicos sobre el articulado

Sobre restricción de acceso y verificación de edad – Artículos 1 a 6

En primer lugar, la restricción de acceso prevista para menores de dieciséis años constituye una medida de protección de alta intensidad frente a riesgos relevantes del entorno digital. Precisamente por esa intensidad, conviene que el Proyecto explicita con mayor detalle su juicio de proporcionalidad, su articulación con alternativas menos restrictivas y su compatibilidad con los derechos de niños, niñas y adolescentes a buscar, recibir y difundir información, expresarse, ser escuchados y participar en entornos digitales seguros, reconocidos en la Ley 1098 de 2006 y en la Convención sobre los Derechos del Niño.

Esta armonización resulta relevante a la luz de los artículos 12,13 y 17 de la Convención de los Derechos del Niño. Estas disposiciones reconocen, respectivamente, el derecho de niños, niñas y adolescentes a ser escuchados en los asuntos que los afectan, a ejercer la libertad de expresión y a acceder a información diversa que favorezca su bienestar, desarrollo y salud. En particular, el artículo 17 no solo ordena protegerlos frente a información y contenidos perjudiciales, sino también promover condiciones positivas de acceso a contenidos de interés para la infancia, incluidos la producción y difusión de materiales adecuados, la cooperación internacional, los libros infantiles y la atención a las necesidades lingüísticas de grupos minoritarios e indígenas. Por ello, el análisis del Proyecto podría considerar no solo medidas de restricción, sino también alternativas de protección diferenciada, como perfiles o configuraciones seguras para menores, usos limitados por funcionalidad, controles frente al contacto con desconocidos, publicidad dirigida, perfilamiento, sistemas de recomendación y mecanismos proporcionados de acompañamiento parental.

En esa línea, sería pertinente que el Proyecto desarrolle con mayor precisión por qué una restricción general por edad resulta idónea, necesaria y proporcional frente a los riesgos identificados, y cómo preserva usos legítimos de información, educación, salud, participación y apoyo para niños, niñas y adolescentes.

Por otro lado, conviene considerar que la verificación robusta de edad puede exigir la recopilación de documentos, datos biométricos u otros identificadores altamente sensibles, creando riesgos adicionales de vigilancia, filtración, suplantación y perfilamiento. Este tema debe analizarse de manera articulada con la Ley 2489 de 2025, que ya regula los entornos digitales sanos y seguros y contempla medidas como verificación de edad, clasificación etaria, controles parentales, advertencias y diseño por defecto. Lo anterior resulta particularmente relevante en atención al principio de proporcionalidad y al deber de evitar duplicidades normativas que puedan generar cargas adicionales sin una evidencia clara sobre su efectividad, de cara, de una parte, a los principios constitucionales de la función administrativa, en particular el principio de eficiencia contenido en el artículo 209 de la Constitución Política y, de otra, a las obligaciones de verificación de identidad y seguridad digital contenidas en la Ley 2573 de 2026. Como se ha señalado desde la CRC, debe darse prioridad a esquemas de verificación de edad o aseguramiento de edad proporcionales según el riesgo que disponga cada servicio o funcionalidad. También convendría prever garantías frente a errores de clasificación, tales como notificación clara, explicación de la decisión, mecanismo sencillo de reclamación, revisión oportuna y restitución rápida de cuentas

cuando corresponda. Esto es relevante frente a falsos positivos, falsos negativos, bloqueo de adolescentes habilitados o exigencias desproporcionadas a adultos.

En relación con el artículo 3, aunque el Proyecto adopta un criterio funcional para definir las redes sociales digitales, algunas de las funcionalidades descritas también pueden estar presentes en servicios audiovisuales, plataformas de video, videojuegos, mensajería, servicios educativos o comunidades cerradas. Por ello, convendría precisar el alcance de la definición y articularla con el proceso técnico previsto en el Decreto 769 de 2026, que asigna al Ministerio TIC, en coordinación con la CRC, la definición y actualización de conceptos técnicos y operativos. Esto permitiría reducir incertidumbres, evitar tratamientos equivalentes para servicios de riesgo distinto y preservar la neutralidad tecnológica..

Sobre protección de datos, sistemas automatizados y riesgos de diseño – Artículos 7 a 9, en concordancia con los artículos 1, 3, 5 y 6

El proyecto identifica riesgos asociados al perfilamiento, la recomendación automatizada y los mecanismos de captación de atención, y sería útil precisar cómo se traducen en obligaciones concretas y verificables. Asimismo, convendría procurar que las medidas de protección no generen una mayor recopilación de datos de NNA ni restricciones desproporcionadas a sus derechos comunicacionales. Para que estas obligaciones sean verificables, sería útil distinguir entre deberes de resultado y deberes de gestión: evaluación de riesgos por funcionalidad, configuración protectora por defecto, límites al perfilamiento y publicidad dirigida a menores, controles sobre reproducción automática, desplazamiento infinito y notificaciones persistentes, mecanismos de denuncia y reportes proporcionales al nivel de riesgo.

La Ley 2489 de 2025 y el Decreto 769 de 2026 ya prevén lineamientos sobre diseño seguro, privacidad, sistemas automatizados, gestión de riesgos y verificación de edad. Por ello, el Proyecto podría precisar cuál es su valor agregado de naturaleza legal y cuáles aspectos deben quedar para desarrollo técnico posterior, evitando duplicidades o mandatos incompatibles. Los lineamientos técnicos sobre algoritmos, diseño de plataformas, gestión de riesgos y mecanismos de verificación se encuentran dentro de las temáticas que pueden desarrollarse vía lineamientos a través de la reglamentación que debe establecer el Ministerio TIC en coordinación con la CRC y, a su vez, es un asunto que esta entidad ha trabajado mediante estudios e interacciones con los agentes interesados, de manera particular en la Agenda Regulatoria 2026-2027 se anunció el «Estudio sobre mecanismos de protección de niñas, niños y adolescentes en medios y servicios audiovisuales» que se publicará en el cuarto trimestre de 2026, por lo que se recomienda considerar la participación de esta Entidad en la reglamentación técnica de la materia.

Respecto al mismo tema de la verificación de edad y otros asuntos que pueden requerir el tratamiento de datos de los NNA, se recomienda revisar la compatibilidad de este proyecto con la Ley 1581 de 2012, así como las recomendaciones señaladas previamente, dirigidas a darle prevalencia a esquemas de verificación de edad acorde al riesgo, con criterios de minimización de datos, proporcionales y que también permitan una gestión de los riesgos de elusión por menores de edad.

El Proyecto de Ley modifica el artículo 7 de la Ley 1581 de 2012 para extender la proscripción del tratamiento hasta los 16 años en redes sociales. Conviene añadir que esa regla debe formularse con cuidado para no impedir tratamientos estrictamente necesarios para protección, seguridad, reclamaciones, verificación proporcional o restablecimiento de derechos.

Sobre obligaciones de diligencia y cumplimiento para las plataformas – Artículos 5 y 17

Conviene valorar los instrumentos prácticos para hacer exigibles las obligaciones frente a proveedores sin presencia física en Colombia, en particular canales de notificación, puntos de contacto, conservación de información, cooperación con autoridades, ejecución de órdenes y criterios de conexión territorial. Lo anterior, ya que, sin un representante legal o responsable de cumplimiento domiciliado en el país, pueden presentarse dificultades para notificar actuaciones, practicar pruebas, requerir información, ejecutar órdenes y hacer efectivas las sanciones. En este sentido, es importante que el Proyecto de Ley tenga en cuenta la jurisprudencia sobre el principio de territorialidad y las competencias y alcances de la Superintendencia de Industria y Comercio en cuanto a empresas no domiciliadas en Colombia.

En el artículo 17, sería conveniente incluir expresamente la participación técnica de la CRC en los asuntos relacionados con estándares, interoperabilidad, gestión de riesgos, diseño de funcionalidades y verificación de edad, manteniendo a la SIC en los ámbitos de protección de datos, consumidor e inspección, vigilancia y control que le correspondan.

También sería conveniente precisar cómo se integrarán estos programas de cumplimiento con las obligaciones ya previstas en la Ley 2489 de 2025 en materia de verificación de edad, controles parentales, auditoría de algoritmos, gestión de riesgos, canales de denuncia y reporte a autoridades, de modo que se evite crear sistemas paralelos de reporte, auditoría y evaluación.

Sobre Inspección, vigilancia y régimen sancionatorio – Artículos 10 a 15

La designación de la SIC como principal autoridad en la materia puede modularse teniendo en cuenta las competencias y experticias del regulador único de las comunicaciones: la CRC, así como las del MinTIC. La SIC puede ejercer funciones de inspección, vigilancia y sanción específicamente en materia de datos personales, siguiendo el ámbito competencial previamente otorgado por la Ley; mientras que la vigilancia y control de otros aspectos relacionados con el cumplimiento de la normativa que se expida, así como respecto de los agentes que emitan ciertos contenidos, podría ser ejercida por MinTIC, en el primer caso, y por la CRC en el segundo, de acuerdo con lo que a continuación se expone:

Vale recordar que en la Ley 2489 de 2025 se estableció la facultad a cargo de MinTIC, en coordinación con la CRC, de establecer políticas y regulaciones relacionadas con el uso seguro de las tecnologías de la información y las comunicaciones a favor de los niños, niñas y adolescentes. Así mismo, allí se determinó que la CRC debe apoyar al MinTIC en los procesos de pedagogía e interlocución relacionados con el objeto y fin de la ley en cita, que no es otro, según lo previamente expresado, que el de promover entornos digitales sanos y seguros para los niños, niñas y adolescentes del país.

Nótese entonces que desde la Ley 2489 de 2025 se reconoció que tanto el MinTIC como la CRC son autoridades que pueden contribuir, dada su experticia técnica, en la temática abordada, con la definición de parámetros técnicos y regulatorios que sirvan al propósito de proteger a los menores en su interacción con los entornos digitales. Fruto de ese trabajo articulado fue expedido el ya mencionado Decreto 769 de 2026, en el que se concretaron, reitérese, una serie de medidas que contribuyen al objetivo ya expuesto.

En este punto cabe recordar que para el MinTIC y la CRC no resulta desconocido el ejercicio de funciones de inspección, vigilancia y control. En el caso de MinTIC, el numeral 11 del artículo 18 de la Ley 1341 de 2009, modificado por el artículo 14 de la Ley 1978 de 2019, prevé que le corresponde a dicha autoridad ejercer las funciones de inspección, vigilancia y control en el sector de Tecnologías de la Información y las Comunicaciones. Entretanto, en el caso de la CRC, los numerales 27 y 30 del artículo 22 de la Ley 1341 de 2009, adicionados por el artículo 19 de la Ley 1978 de 2019, le otorgaron facultades de inspección, vigilancia y control respecto de los contenidos que se emiten en el servicio público de televisión.

Dado que, según lo expuesto, la Ley 1341 y la Ley 2489 han dado a MinTIC funciones de inspección, vigilancia y control en el sector TIC y para el desarrollo de políticas y regulaciones para la protección de menores en entornos digitales, no puede pasarse por alto que tal entidad tiene la experticia para ampliar sus funciones de inspección, vigilancia y control al cumplimiento de la normativa que se expida por cuenta del proyecto en análisis.

En atención a lo definido en la Ley 2489 de 2025, la CRC ha ofrecido su conocimiento técnico y regulatorio para contribuir al fortalecimiento del marco normativo que propende por la protección de niños, niñas y adolescentes. En ese contexto, podría evaluarse la conveniencia de fortalecer y articular el papel de la CRC en los entornos digitales, aprovechando la experiencia que ha desarrollado en la inspección, vigilancia y control de contenidos audiovisuales en el servicio público de televisión y en la garantía de los derechos de las audiencias, para que pueda ejercer funciones equivalentes frente a determinados contenidos difundidos en entornos digitales que puedan afectar los derechos de los menores. Una decisión de esta naturaleza permitiría avanzar hacia un esquema de protección más coherente entre medios tradicionales y entornos digitales, sujeto, naturalmente, a la delimitación expresa que establezca el legislador sobre su alcance, sujetos obligados y mecanismos de intervención.

En suma, no puede perderse de vista que cualquier normatividad dirigida a asegurar niveles de protección en entornos digitales, no comporta solamente una vigilancia respecto a los riesgos frente a la privacidad y los datos personales de menores, sino también la vigilancia respecto a que los diferentes actores garanticen un cuidado de todos los derechos fundamentales de los niños, como son la libertad de expresión, la vida, su integridad física y moral, evitando o minimizando los riesgos de acceso a contenidos ilegales o ilícitos. Estos riesgos superan la competencia de la SIC, y podrían ser abordados por el MinTIC como entidad de vigilancia del sector TIC, y por la CRC como entidad de vigilancia frente a tales contenidos.

Conviene considerar, además, que un régimen sancionatorio puede enfrentar desafíos de efectividad frente a proveedores sin presencia jurídica o patrimonial en Colombia. En este sentido, podría ser útil evaluar durante el trámite del presente Proyecto de Ley si la iniciativa prevé instrumentos suficientes para ejecutar órdenes, recaudar multas y obtener información de plataformas establecidas en el exterior.

Las órdenes de suspensión de funcionalidades o modificación de mecanismos técnicos deberían sujetarse a criterios de motivación, necesidad, temporalidad, proporcionalidad y revisión, para evitar efectos equivalentes a bloqueos generalizados o restricciones injustificadas al acceso a información lícita.

Sobre corresponsabilidad y política pública de protección digital – Artículos 16 y 17

Resulta pertinente considerar que la Ley 2489 de 2025 ya creó un marco de política pública y la posibilidad de establecer reglamentación respecto a entornos digitales seguros con la corresponsabilidad como eje central que distribuye responsabilidades y apoyo entre los actores. Por ello, convendría valorar la articulación de cualquier nueva política con dicho marco, con el fin de prevenir posibles fragmentaciones de la acción estatal, duplicidades de funciones o inconsistencias institucionales.

Esta articulación debería considerar los instrumentos ya previstos en la Ley 2489 de 2025 y el Decreto 769 de 2026: Comité Nacional de Tecnología, Niñez y Adolescencia, mesas técnicas, repositorio de buenas prácticas, informes anuales y Sistema Integral de Monitoreo, Evaluación y Desarrollo Tecnológico. Así, la nueva política no operaría como un régimen paralelo, sino como un refuerzo del marco vigente.

También sería útil prever indicadores de seguimiento que no se limiten al número de cuentas bloqueadas o eliminadas, sino que midan uso efectivo, evasión, desplazamiento a servicios no cubiertos, reclamaciones, errores de clasificación, tiempos de respuesta, incidentes de privacidad y efectos sobre acceso a educación, salud, participación e información.

3. Conclusiones y recomendaciones

A partir de los aportes y evidencias desarrollados en este documento, la CRC se permite sintetizar los principales puntos para que sean tenidos en cuenta por los autores del presente proyecto de Ley, en aras de su fortalecimiento y articulación funcional.

(i) La protección de los niños, niñas y adolescentes en línea admite instrumentos regulatorios de distinta intensidad y no existe un modelo único. La experiencia comparada combina diseño seguro, configuraciones protectoras, gestión de riesgos y condiciones de acceso según el riesgo, la funcionalidad y el grupo etario involucrados, lo cual resulta coherente con el enfoque diferenciado de la Ley 2489 de 2025 y del Decreto 769 de 2026.

(ii) Identificar correctamente que un usuario es menor de edad permite activar las protecciones que le corresponden, pero deja pendientes las condiciones bajo las cuales utiliza el servicio. Los

sistemas de recomendación, el contacto con desconocidos, la publicidad dirigida y determinadas características de diseño pueden seguir generando riesgos aun cuando la plataforma conozca su edad. En ese sentido, la garantía de edad cumple una función instrumental dentro de un esquema más amplio de protección. Su aplicación debe vincularse con medidas de prevención y mitigación sobre el funcionamiento de las plataformas, de manera que el control de acceso complemente la gestión del riesgo y no se convierta en su sustituto.

(iii) La eficacia de la garantía de edad depende de su precisión, oportunidad, privacidad y resistencia a la evasión. Ningún método elimina por completo los errores de clasificación ni la evasión, y acreditar un umbral de edad no exige identificar plenamente al usuario. Por ello, resulta conveniente contemplar niveles de desempeño verificables, minimización de datos y procedimientos de reclamación y corrección acordes con el riesgo.

(iv) La evidencia disponible sobre prohibiciones generales muestra cambios en la tenencia formal de cuentas, pero todavía no demuestra en igual medida una reducción del daño. En Australia, la disminución de cuentas fue mayor que la del uso efectivo, y la propia autoridad advierte que es temprano para evaluar resultados de largo plazo. La evaluación debería distinguir entre la aplicación de la medida, los cambios de comportamiento y los resultados de protección, sin presumir relaciones causales que aún no han sido demostradas.

(v) Cuanto más general e intensa es la restricción, mayor es la carga de justificar su focalización y su necesidad, así como la valoración de alternativas menos restrictivas. Esa justificación debe extenderse a la infraestructura utilizada para hacerla efectiva: qué información requiere, quién la trata, cómo se corrigen los errores y con qué capacidades se supervisa. De este modo, para el presente proyecto de Ley, es importante asegurar que los medios sean proporcionales al beneficio esperado, se articulen con las competencias e instrumentos existentes y permitan verificar resultados y ajustar las medidas conforme avance la evidencia.

La CRC reitera su disposición para aportar, en el marco de sus competencias, los elementos técnicos y regulatorios que resulten pertinentes durante la discusión de la iniciativa y para contribuir a la construcción de un marco normativo coherente, efectivo y sostenible para la protección de los niños, niñas y adolescentes en los entornos digitales.

Con base a lo anterior, nos ponemos a su disposición para realizar una mesa de trabajo en la cual podemos ampliar y aportar activamente a la construcción de esta importante iniciativa legislativa.

Cordialmente,

DÍAZ SUAZA
FELIPE
AUGUSTO

Firmado digitalmente por
DÍAZ SUAZA FELIPE
AUGUSTO
Fecha: 2026.10.06 10:36:48
-05'00'

FELIPE AUGUSTO DÍAZ SUAZA

Director Ejecutivo CRC

Proyectado por: Sergio A. Urquijo

Revisado por: Víctor Baldrich

Aprobado por: Zoila Vargas



@CRCCol



/CRCCol



/CRCCol



CRCOL



@CRCCol

Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, piso 9 Bogotá, D.C.
Código postal 110231 - Teléfono +57 601 319 8300
Línea gratuita nacional 018000 919278