

INFANCIAS Y ENTORNOS DIGITALES: TENDENCIAS REGULATORIAS EN AMÉRICA LATINA

Derechos Digitales
AMÉRICA LATINA

INFANCIAS Y ENTORNOS DIGITALES:
TENDENCIAS REGULATORIAS EN AMÉRICA LATINA

Esta publicación fue realizada por Derechos Digitales, organización independiente sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales en América Latina.

Esta publicación fue posible gracias al apoyo de Luminate.

Supervisión general y revisión: Jamila Venturini

Investigación, análisis y redacción: Marina Meira

Revisión de estilo: Gastón Wahnish

Diseño: Alter Studio

NOVIEMBRE, 2026

Cómo citar esta publicación: Derechos Digitales. (2026). Infancias y entornos digitales: tendencias regulatorias en América Latina. https://www.derechosdigitales.org/recursos/infancias-y-entornos-digitales-tendencias-regulatorias-en-america-latina/

CC-BY 4.0
Esta obra está disponible bajo licencia Creative Commons Atribución 4.0 Internacional
https://creativecommons.org/licenses/by/4.0/deed.es

ÍNDICE

INTRODUCCIÓN 4

1. ANTECEDENTES 6

1.1. Marcos penales y sus tensiones 9

1.2. La Observación General 25 del Comité de los Derechos del Niño de las Naciones Unidas como marco basado en derechos 12

1.3. Modelos regulatorios dirigidos a servicios digitales 13

2. TENDENCIAS LEGISLATIVAS EN AMÉRICA LATINA PARA LA PROTECCIÓN Y PROMOCIÓN DE DERECHOS DE NNA EN ENTORNOS DIGITALES 17

2.1. Argentina 18

2.2. Bolivia 20

2.3. Brasil 21

2.4. Chile 23

2.5. Colombia 25

2.6. Ecuador 27

2.7. México 29

2.8. Panamá 31

2.9. Paraguay 32

2.10. Perú 34

2.11. Uruguay 35

3. PRINCIPALES TENDENCIAS REGULATORIAS EN LA REGIÓN 38

3.1. Expansión de la respuesta penal y de la vigilancia 38

3.2. Restricciones etarias y la expansión de la determinación de edad 42

3.3. De restringir el acceso a regular los servicios digitales 46

3.4. Dos agendas emergentes: participación en actividades económicas digitales e inteligencia artificial 47

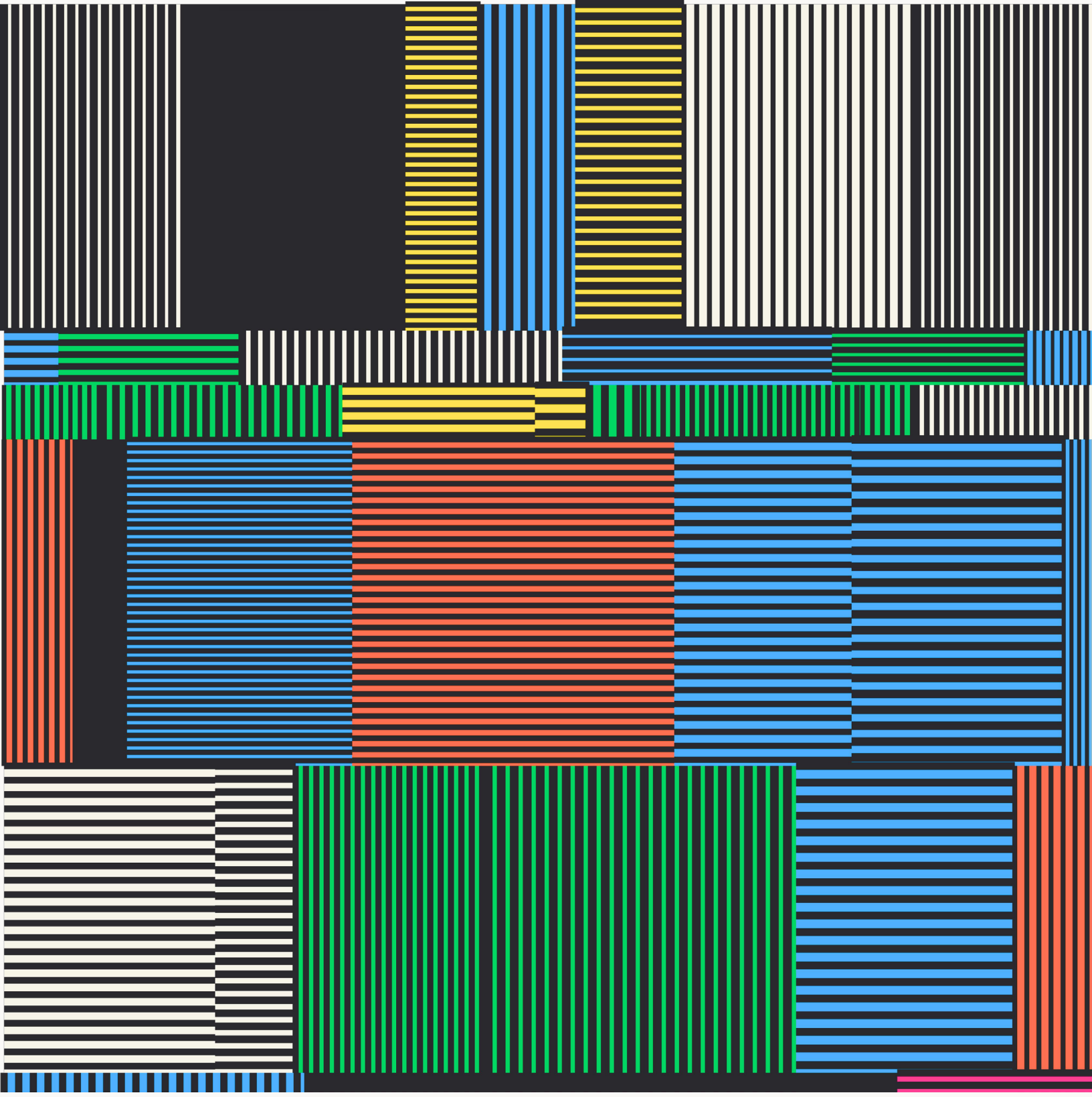
4. CONSIDERACIONES FINALES 51

INTRODUCCIÓN

Esta publicación presenta un panorama de las principales tendencias legislativas sobre la protección de niñas, niños y adolescentes (NNA) en entornos digitales en América Latina. A partir de leyes, reglamentaciones y proyectos de ley identificados entre junio de 2024 y septiembre de 2026 en 11 países, busca reconocer los riesgos que orientan estas respuestas y los distintos modelos regulatorios adoptados o propuestos. El análisis toma como referencia los derechos humanos, considerando tanto los derechos de NNA como las implicaciones de estas medidas para el conjunto de las personas usuarias de internet.

El informe no pretende ofrecer un inventario exhaustivo de las iniciativas de la región ni evaluar los resultados de implementación de las normas. Se concentra en iniciativas de alcance nacional directamente relacionadas con la protección de NNA en entornos digitales. Quedan fuera las medidas centradas exclusivamente en el uso de dispositivos en establecimientos educativos y los marcos generales de protección de datos o inteligencia artificial cuyo objeto principal no es esta protección.

La publicación se organiza en cuatro partes. Primero, presenta los antecedentes y los marcos de referencia del debate. Luego, describe las iniciativas identificadas por país y analiza las principales tendencias regionales, que incluyen el refuerzo de respuestas penales, restricciones etarias de acceso a redes sociales, regulaciones más amplias de servicios digitales y las agendas emergentes relacionadas a la participación económica de NNA en entornos digitales e inteligencia artificial (IA). Después identifica las principales tendencias regionales para, finalmente, plantear consideraciones para orientar una agenda latinoamericana que garantice una protección integral basada en derechos.



01

ANTECEDENTES

01

01. ANTECEDENTES

La protección de niñas, niños y adolescentes (NNA) en entornos digitales ha adquirido en los últimos años una presencia creciente en las agendas regulatorias y de políticas públicas de América Latina y de otras regiones del mundo. Este proceso acompaña, en primer lugar, una tendencia más amplia de expansión del acceso y uso de internet que también alcanza a las generaciones más jóvenes. Niñas, niños y adolescentes acceden a internet desde edades cada vez más tempranas y utilizan tecnologías digitales para actividades diversas, que van desde estudiar y buscar información hasta comunicarse, jugar y acceder a contenidos audiovisuales.

Ya en 2017, UNICEF estimaba que una de cada tres personas usuarias de internet en el mundo tenía menos de 18 años. En América Latina, la expansión de la conectividad durante los últimos años ha profundizado esta tendencia. Un estudio publicado por la CEPAL en junio de 2026, basado en datos comparables de la iniciativa Kids Online en Argentina, Bolivia, Brasil, Chile, Costa Rica y Uruguay, muestra que el acceso a internet en el hogar supera actualmente el 90% en la mayoría de esos países. El teléfono móvil se ha consolidado, además, como el principal dispositivo de conexión y se adquiere a edades cada vez más tempranas. Las prácticas más extendidas entre NNA en la internet incluyen el entretenimiento audiovisual, la comunicación interpersonal y el aprendizaje informal, con una presencia destacada de plataformas de mensajería y de redes sociales como WhatsApp, YouTube y TikTok[1].

Estos datos, sin embargo, no describen una experiencia homogénea. Hablar de la relación entre infancia y tecnologías en América Latina requiere considerar las profundas desigualdades que caracterizan a la región. Las condiciones socioeconómicas, el territorio, el género, la raza y etnia, las condiciones de acceso a la educación y las estructuras familiares y de cuidado inciden tanto en las posibilidades de acceso a las tecnologías como en las formas en que estas son utilizadas y mediadas. En este sentido, resulta más apropiado hablar de *infancias* y sus distintas relaciones con entornos digitales, en plural[2].

1 Magdalena Claro, Patricio Cabello y Carolina Castro Grau. *Experiencia digital en la niñez y adolescencia en América Latina: Argentina, Bolivia (Estado Plurinacional de), Brasil, Chile, Costa Rica y Uruguay.* CEPAL. (Santiago, 2026). Disponible en: https://www.cepal.org/es/publicaciones/90132-experiencia-digital-la-ninez-adolescencia-america-latina-argentina-bolivia

2 Isabella Henriques, Marina Meira y Pedro Hartung. "As múltiplas infâncias e a invisibilidade da criança", *O Futuro da Infância no Mundo Digital*. (São Paulo, 2021), 237-243. Disponible en: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/o-futuro-da-infancia-no-mundo-digital-ensaios-sobre-liberdade-seguranca-e-privacidade.pdf

Es decir, las experiencias de niñas y niños difieren según sus condiciones sociales, económicas, culturales y territoriales, y esas desigualdades se trasladan también a su relación con el entorno digital. La evidencia regional, por su turno, confirma la persistencia de estas diferencias. Aunque el acceso doméstico a internet se aproxima a niveles elevados en los seis países analizados por la CEPAL, siguen existiendo brechas socioeconómicas importantes, particularmente en el acceso a computadoras y otros dispositivos que permiten usos más diversificados y complejos[3].

Las desigualdades también atraviesan las posibilidades de acompañamiento familiar. Estudios nacionales de la serie Kids Online han mostrado asociaciones entre las condiciones socioeconómicas y educativas de los hogares y las formas de mediación del uso de internet. En general, la escolaridad de madres, padres y responsables familiares está asociada con las acciones de orientación y mediación de la experiencia digital de sus hijos e hijas[4]. Esto resulta particularmente relevante en una región marcada por altos niveles de informalidad laboral, desigual distribución del trabajo de cuidados y limitaciones de tiempo y recursos en muchos hogares. Estas condiciones no determinan por sí solas las prácticas digitales de NNA, pero forman parte del contexto en el que las familias pueden (o no) acompañar esas experiencias.

La expansión del acceso a entornos digitales también ha venido acompañada de una creciente preocupación por los riesgos que NNA pueden enfrentar en internet. Por encontrarse en etapas de desarrollo físico, cognitivo y psicosocial, NNA pueden ser particularmente susceptibles a determinadas formas de manipulación, explotación, violencia y prácticas comerciales, con características y niveles de exposición que varían según la edad, la evolución de sus capacidades y sus contextos individuales y sociales.

La tipología desarrollada por la OCDE permite dimensionar la complejidad de esos riesgos, organizándolos en cuatro grandes categorías: contenido, conducta, contacto y consumo[5]. Los primeros se refieren a la exposición a contenidos que pueden resultar nocivos, ilegales o inadecuados, como discursos de odio, desinformación o determinados contenidos violentos o sexuales. Los riesgos de conducta surgen de las propias interacciones entre NNA en entornos digitales e incluyen, por ejemplo, situaciones de ciberbullying, inter-

3 Magdalena Claro, Patricio Cabello y Carolina Castro Grau. *Experiencia digital en la niñez y adolescencia en América Latina: Argentina, Bolivia (Estado Plurinacional de), Brasil, Chile, Costa Rica y Uruguay. CEPAL. (Santiago, 2026). Disponible en:* https://www.cepal.org/es/publicaciones/90132-experiencia-digital-la-ninez-adolescencia-america-latina-argentina-bolivia

4 Ibid

5 OECD. *Children in the digital environment: revised typology of risks*. (Paris, 2021). Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf

cambios de contenido sexual entre pares y otras conductas potencialmente perjudiciales. Los riesgos de contacto, en cambio, se producen en interacciones con personas adultas que pueden exponer a NNA a situaciones de acoso, manipulación, abuso o explotación sexual. Finalmente, los riesgos de consumo están relacionados con su participación como personas usuarias y consumidoras de servicios digitales e incluyen, entre otros, prácticas comerciales inapropiadas, perfilamiento comercial, fraudes y gastos inducidos.

Estas categorías no operan de forma aislada y se intersectan con otros derechos humanos. Una misma experiencia puede combinar riesgos de contenido, contacto, conducta, consumo y privacidad, mientras que determinadas características del diseño de servicios digitales pueden contribuir a amplificarlos. Sistemas de recomendación en redes sociales pueden aumentar la exposición reiterada a ciertos contenidos inadecuados; mecanismos orientados a maximizar la interacción pueden incentivar determinados comportamientos dañinos; y la recolección de datos para el perfilamiento puede exponerlos a prácticas de explotación comercial como la publicidad dirigida.

Esta multidimensionalidad es relevante para comprender la creciente atención regulatoria al tema, pero también para analizar críticamente las respuestas que vienen siendo propuestas. Si los riesgos que afectan a NNA tienen causas diferentes, se combinan entre sí y están atravesados por condiciones sociales y económicas más amplias, difícilmente pueden ser enfrentados mediante una única medida tecnológica o jurídica.

La creciente centralidad política del tema también se explica por una acumulación progresiva de evidencia sobre estos riesgos. Otra razón es que, en distintos países, casos graves de violencia, abuso o muerte de NNA relacionados de alguna manera con el uso de servicios digitales han adquirido una fuerte repercusión pública y contribuido a acelerar debates regulatorios. Estos episodios cumplen muchas veces una función catalizadora de hacer visibles riesgos hasta entonces poco discutidos y generar presión para que los poderes públicos respondan. Al mismo tiempo, el contexto de urgencia y conmoción que los rodea puede favorecer respuestas legislativas reactivas y concentradas en el riesgo que adquirió mayor visibilidad pública, aun cuando este constituya solamente una dimensión de un problema más amplio.

Esta creciente atención política también se expresa en espacios de articulación regional. El 20 de diciembre de 2025, Argentina, Bolivia, Brasil, Paraguay y Uruguay —en cuanto Estados Partes y Asociados del MERCOSUR— adoptaron una declaración sobre protección de NNA en entornos digitales[6]. El documento reconoce la autonomía progresiva y la importancia de las tecnologías para el ejercicio de derechos, e insta a las empresas a

6 Declaración especial del MERCOSUR sobre protección de la infancia y adolescencia en entornos digitales. 20 de diciembre de 2025. Disponible en: www.mercosur.int/declaracion-especial-del-mercosur-sobre-proteccion-de-la-infancia-y-adolescencia-en-entornos-digitales

adoptar altos niveles de seguridad desde el diseño y protección de la privacidad. También promueve la cooperación para investigar delitos, atender a las víctimas y fortalecer capacidades institucionales, y subraya que las salvaguardas ofrecidas por los servicios digitales no deben ser asimétricas entre países. La declaración refleja así la incorporación del tema a una agenda regional que abarca tanto las responsabilidades empresariales como la actuación coordinada de los Estados.

Asimismo, la relación entre NNA y tecnologías no debe ser abordada únicamente desde el riesgo. Internet y las tecnologías digitales constituyen espacios para el ejercicio de derechos, incluyendo el acceso a la información y a la educación, la libertad de expresión, la participación, el juego, la cultura y la socialización. Una política orientada a la protección debe, por lo tanto, ser capaz de reducir riesgos sin eliminar las oportunidades y derechos asociados al acceso y participación de NNA en entornos digitales.

La Convención sobre los Derechos del Niño[7] parte del reconocimiento de niñas, niños y adolescentes como sujetos y titulares de derechos humanos, que deben ser garantizados también a lo largo de las distintas etapas de su desarrollo. Al mismo tiempo, su condición particular de desarrollo fundamenta el derecho a medidas especiales de protección y cuidado, que deben acompañar la evolución de sus capacidades y su autonomía progresiva. Esta doble dimensión —el pleno ejercicio de derechos y la garantía de una protección especial— resulta central para abordar su relación con los entornos digitales y evitar que NNA sean tratados únicamente como objetos de protección, en lugar de como sujetos de derechos que deben poder ejercerlos y disfrutarlos plenamente también en estos espacios.

1.1. Marcos penales y sus tensiones

La preocupación legislativa por los riesgos que las tecnologías pueden representar para NNA no es nueva en América Latina. Mucho antes de la actual proliferación de iniciativas legales, varios países de la región habían reformado sus legislaciones penales para responder a formas de violencia —especialmente sexual— facilitadas por tecnologías, particularmente la producción y circulación de material de abuso sexual infantil y el *grooming*, entendido como el acercamiento de una persona adulta a NNA a través de medios digitales con fines sexuales.

Argentina, por ejemplo, tipificó en 2013, mediante la Ley 26.904[8], el contacto con NNA por medios electrónicos con el propósito de cometer delitos contra su integridad sexual.

7 Disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf

8 Disponible en: https://www.argentina.gob.ar/normativa/nacional/223586/texto

Perú aprobó el año siguiente la Ley 30.171[9], que incorporó a su legislación penal las proposiciones a NNA con fines sexuales realizadas a través de internet u otros medios tecnológicos. Costa Rica, por su parte, adoptó en 2021 la Ley 10.020[10] para prevenir y sancionar el *grooming*, reformando distintas disposiciones de su Código Penal y creando además una comisión interinstitucional dedicada a la materia. Una comparación regional publicada por ECPAT en 2022 identificaba entonces cinco países latinoamericanos (Colombia, Costa Rica, Honduras, Perú y Uruguay) cuyas legislaciones criminalizaban expresamente el grooming con fines sexuales, incluso mediante internet y otras tecnologías de la información y comunicación, además de otros siete que lo hacían parcialmente[11].

Brasil siguió una trayectoria relacionada, aunque con instrumentos diferentes. Además de las disposiciones del Estatuto da Criança e do Adolescente que criminalizan conductas relacionadas con la producción, difusión y posesión de material de abuso sexual infantil, en 2017 la Ley 13.441[12] autorizó la infiltración de agentes policiales en internet para investigar determinados delitos contra la dignidad sexual de NNA.

Este conjunto de antecedentes permite identificar una característica importante de las primeras respuestas estatales a la relación entre infancia e internet: su fuerte concentración en el derecho penal y, particularmente, en la violencia y explotación sexual. En una etapa todavía inicial de desarrollo de marcos jurídicos dirigidos específicamente a conductas realizadas o facilitadas en entornos digitales en América Latina, estas respuestas se orientaron principalmente a adaptar tipos penales y herramientas de investigación existentes, o a crear otros nuevos, para responder a las formas que estas conductas adquirían con el uso de tecnologías digitales.

Algunas de estas respuestas también generaron tensiones con otros derechos y garantías vinculados al uso de internet. Con el tiempo, estas controversias contribuyeron a construir una pretensa oposición entre dos agendas que deberían ser complementarias: la protección de NNA en entornos digitales y la defensa de los derechos humanos en internet. El debate sobre criptografía constituye un ejemplo particularmente claro. En distintos países, el combate al abuso y la explotación sexual de NNA y a la circulación

9 Disponible en: https://img.lpderecho.pe/wp-content/uploads/2023/07/Ley-30171-LPDerecho.pdf

10 Disponible en: https://vlex.co.cr/vid/asamblea-legislativa-republica-costa-915230449

11 ECPAT. *Latin America – Summary of Recommendations: Legal Interventions in Latin America*. (2022). Disponible en: https://ecpat.org/resource/latin-america-summary-of-recommendations-legal-interventions-in-latin-america/

12 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm

de material de abuso sexual infantil ha sido utilizado como argumento para proponer mecanismos que permitan acceder o escanear comunicaciones privadas, debilitando las garantías ofrecidas por la criptografía de extremo a extremo[13]. El debate suele plantearse como una elección entre la seguridad de NNA y la protección de la privacidad. Esta formulación, sin embargo, parte de una premisa equivocada[14]. La criptografía también protege a NNA, al preservar la confidencialidad de sus comunicaciones, contribuir a su seguridad y posibilitar el ejercicio de derechos como la privacidad y la libertad de expresión. Al mismo tiempo, su debilitamiento tiene implicaciones que exceden este grupo, ya que afecta una tecnología fundamental para la seguridad y la confianza en el ecosistema digital, utilizada para proteger comunicaciones, transacciones, datos personales y múltiples servicios e infraestructuras frente a accesos no autorizados. Medidas adoptadas para responder a un riesgo específico pueden, de este modo, introducir vulnerabilidades con consecuencias para el conjunto de las personas usuarias de internet.

Tensiones similares aparecen frente a la adopción masiva de tecnologías de vigilancia en espacios públicos justificadas por objetivos de protección de NNA. Tecnologías como el reconocimiento facial, por ejemplo, han sido presentadas como herramientas para contribuir a la identificación y localización de NNA desaparecidos. Aunque el objetivo de localizar a NNA desaparecidos es indiscutiblemente legítimo, no existe evidencia suficiente de que el despliegue de sistemas de reconocimiento facial constituya una respuesta efectiva y necesaria para alcanzarlo. En cambio, existe evidencia documentada sobre los riesgos y daños asociados a estas tecnologías, incluidos errores de identificación, impactos discriminatorios (particularmente sobre personas negras y otros grupos históricamente sujetos a vigilancia), detenciones indebidas y la expansión de infraestructuras de vigilancia masiva[15]. En América Latina, donde sistemas de reconocimiento facial ya han sido desplegados para fines de seguridad pública y vigilancia urbana, ampliar estas infraestructuras en nombre de la protección de NNA puede contribuir a normalizar tecnologías cuyos impactos sobre la privacidad, la no discriminación

13 Child Rights International Network, defenddigitalme. Privacy and Protection: A children's rights approach to encryption. (United Kingdom, 2023). Disponible en: https://home.crin.org/readlistenwatch/stories/privacy-and-protection

14 Meira, M. & Amaral, P., "As falhas da oposição entre criptografia e proteção de crianças e adolescentes", *(2023). Disponible en:* https://obcrypto.org/as-falhas-da-oposicao-entre-criptografia-e-protecao-de-criancas-e-adolescentes/

15 ALSUR, *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa.* (2021). Disponible en: https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia; ALSUR, *Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales*. (2025). Disponible en: https://www.alsur.lat/reporte/reconocimiento-facial-tecnologias-vigilancia-en-america-latina-casos-proveedores-dinamicas

y otros derechos humanos ya se encuentran documentados.

Estos ejemplos no implican negar los problemas que estas medidas buscan enfrentar. Por el contrario, muestran por qué la gravedad de los riesgos que afectan a NNA exige evaluar con especial cuidado la efectividad y los impactos de las respuestas legales y de políticas públicas propuestas. Tampoco resulta productivo tratar la protección de NNA y la defensa de los derechos humanos en internet como agendas enfrentadas. Esta oposición puede llevar, de un lado, a que preocupaciones legítimas sobre privacidad, seguridad o libertad de expresión sean presentadas como obstáculos a la protección de la infancia y, de otro, a que medidas destinadas a proteger a NNA sean analizadas exclusivamente a partir de sus posibles efectos restrictivos, sin considerar adecuadamente los riesgos y violencias que buscan enfrentar.

1.2. La Observación General 25 del Comité de los Derechos del Niño de las Naciones Unidas como marco basado en derechos

Este conjunto de tensiones ayuda a comprender el surgimiento de un enfoque más amplio sobre la relación entre NNA y los entornos digitales. Frente a una generación anterior de respuestas centradas principalmente en la criminalización de determinadas conductas y en la protección frente a riesgos específicos, comenzó a consolidarse una perspectiva orientada a pensar el entorno digital desde el conjunto de los derechos de NNA. Este cambio no supuso abandonar las respuestas frente a formas graves de violencia, pero sí ampliar el marco de análisis, incorporando también las condiciones necesarias para que NNA puedan ejercer sus derechos y participar de los entornos digitales de manera segura y acorde con su autonomía progresiva.

El hito central en este proceso fue la adopción, en 2021, de la Observación General 25 sobre los derechos de la niñez en relación con el entorno digital[16], por el Comité de los Derechos del Niño de las Naciones Unidas. El documento interpreta las obligaciones establecidas por la Convención sobre los Derechos del Niño frente a las transformaciones producidas por las tecnologías digitales y establece que los Estados deben respetar, proteger y hacer efectivos los derechos de NNA también en estos entornos. Su elaboración incluyó un proceso de consulta en el que participaron más de 700 NNA y jóvenes de 27 países.

La relevancia de la Observación General 25 radica, entre otros aspectos, en desplazar el debate de una lógica exclusivamente orientada a proteger a NNA de internet hacia una discusión sobre cómo garantizar sus derechos en el entorno digital. El documento reconoce tanto los riesgos como las oportunidades asociadas a las tecnologías y sitúa

16 Disponible en: https://docs.un.org/es/crc/c/gc/25

principios de la Convención, como el interés superior, la no discriminación, la autonomía progresiva y el desarrollo de las capacidades y el derecho a ser escuchados, en el centro de las políticas digitales. El texto apunta que el acceso significativo a tecnologías puede contribuir al ejercicio de derechos civiles, políticos, económicos, sociales y culturales. Las medidas de protección, por lo tanto, deben ser evaluadas también a la luz de sus posibles impactos sobre esos derechos.

Al mismo tiempo, la Observación General proporciona un marco de referencia para traducir los principios y obligaciones de la Convención a la formulación de políticas públicas y marcos regulatorios sobre tecnologías digitales. Al abordar cuestiones como protección de datos y privacidad, prácticas comerciales, diseño de servicios, acceso a contenidos, seguridad, alfabetización digital y responsabilidades del sector empresarial, el documento ofrece una base normativa común a partir de la cual los Estados pueden desarrollar respuestas regulatorias concretas. En este sentido, su adopción no solo contribuyó a consolidar un enfoque de derechos sobre la relación entre infancia y tecnologías, sino que también se convirtió en un antecedente relevante para la nueva generación de políticas y regulaciones dirigidas a NNA en entornos digitales.

1.3. Modelos regulatorios dirigidos a servicios digitales

De forma paralela a la consolidación de este marco internacional de derechos, comenzaron a multiplicarse iniciativas regulatorias dirigidas a la relación de NNA con servicios y entornos digitales. Este movimiento se desarrolló en la confluencia de una creciente incorporación de un enfoque de derechos de NNA en el entorno digital, impulsada, entre otros instrumentos, por la Observación General 25, y del avance de marcos integrales de regulación de plataformas digitales.

Este movimiento adquirió inicialmente mayor intensidad en países del Norte Global, particularmente en Europa y Australia. En estos contextos, las respuestas regulatorias fueron más allá del abordaje de conductas ilícitas y comenzaron a incorporar medidas orientadas a intervenir sobre las características y prácticas de los propios servicios digitales. Así, adquirieron mayor relevancia las obligaciones dirigidas a las empresas, incluyendo aquellas relacionadas con el tratamiento de datos personales y con el diseño y funcionamiento de productos y servicios digitales.

Uno de los primeros referentes de esta nueva generación regulatoria fue el *Age Appropriate Design Code* del Reino Unido[17], desarrollado por el Information

17 Disponible en: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

Commissioner's Office (ICO). Su elaboración respondió a un mandato establecido por la Data Protection Act de 2018, que encargó al ICO la adopción de un código de práctica específico sobre estándares de diseño apropiados para la edad en servicios de la sociedad de la información susceptibles de ser utilizados por NNA. El Código estableció 15 estándares para servicios digitales con probabilidad de ser utilizados por NNA, incluyendo la consideración del interés superior de NNA, configuraciones de alta privacidad por defecto, minimización de datos, limitaciones al perfilamiento y la geolocalización y restricciones al uso de técnicas de diseño destinadas a inducirlos a proporcionar datos personales innecesarios o reducir sus protecciones de privacidad.

El marco regulatorio británico se amplió posteriormente con el *Online Safety Act*[18], que establece obligaciones para servicios de interacción entre personas usuarias, motores de búsqueda y determinados servicios que publican contenidos pornográficos, con requisitos diferenciados según el tipo de servicio y los riesgos involucrados. En 2025, el Office of Communications (Ofcom) —autoridad reguladora para la radiodifusión, internet, telecomunicaciones y servicios postales[19]—, publicó los códigos de práctica específicos para la protección de NNA aplicables a servicios de interacción entre personas usuarias y motores de búsqueda, profundizando así una aproximación regulatoria que, además de las garantías vinculadas a la privacidad y al diseño, incorpora obligaciones de evaluación y mitigación de riesgos por parte de los proveedores.

En paralelo, a nivel de la Unión Europea, la aprobación del *Digital Services Act (DSA)*[20] en 2022 incorporó la protección de NNA al marco general de regulación de los servicios digitales. A diferencia del Código británico, el DSA no es una normativa específicamente dirigida a NNA, sino un marco general de regulación de los servicios digitales que incorpora disposiciones específicas para su protección. Entre ellas, está la exigencia de que las plataformas accesibles a NNA adopten medidas apropiadas y proporcionadas para garantizar un alto nivel de privacidad, seguridad y protección en sus servicios. También prohíbe presentarles publicidad basada en perfilamiento a partir de sus datos personales cuando la plataforma conoce con razonable certeza la edad de la persona usuaria. Estas disposiciones reflejan algunos de los debates presentes también en la Observación General 25, particularmente en relación con el tratamiento de datos personales y las prácticas comerciales dirigidas a NNA.

Australia, por otro lado, cuenta con una trayectoria propia de regulación de la seguridad

18 Disponible en: https://www.legislation.gov.uk/ukpga/2023/50/contents

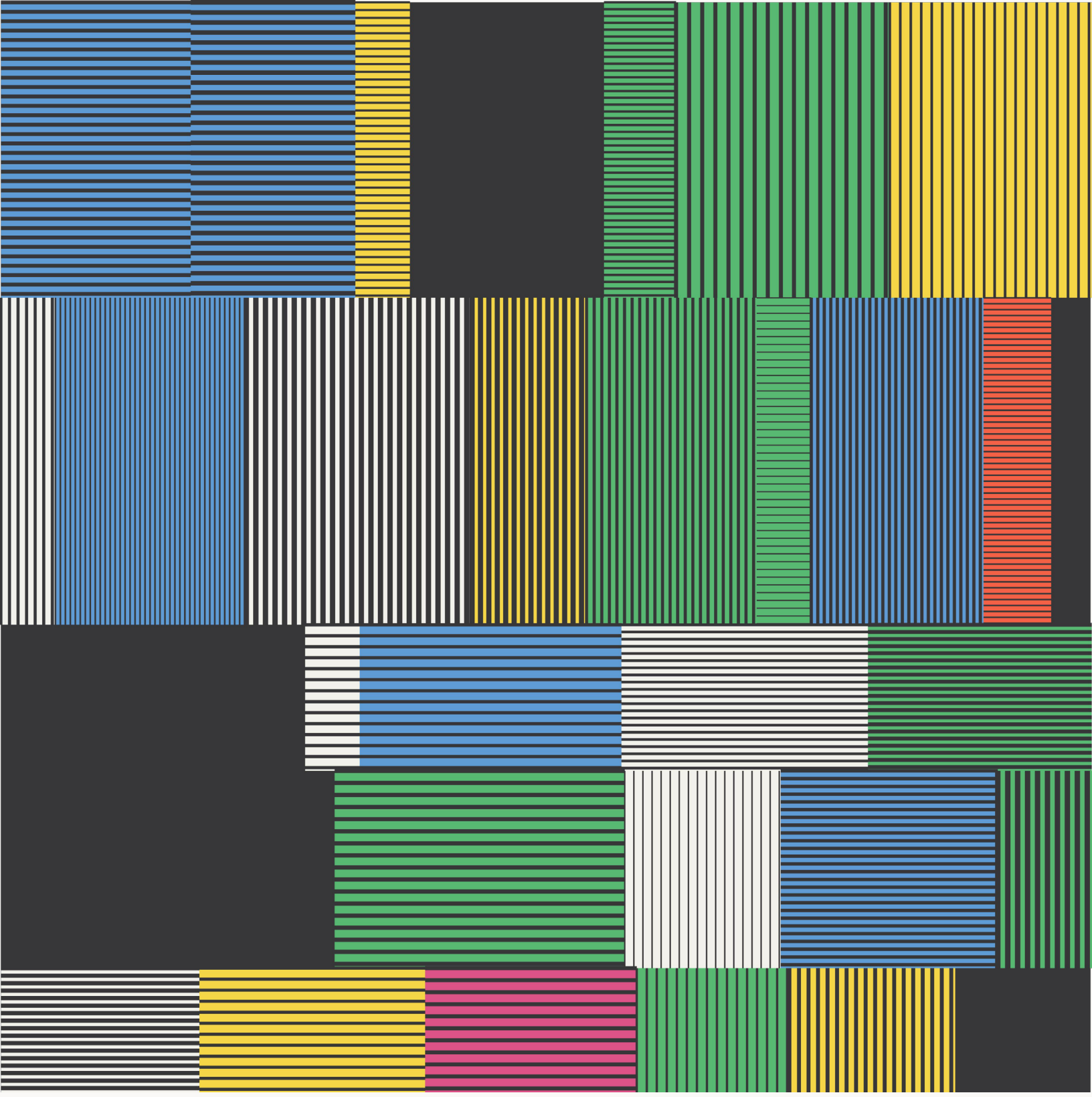
19 Disponible en: https://www.ofcom.org.uk/

20 Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2065

en línea. En 2015 creó el *eSafety Commissioner* —la autoridad independiente responsable de la seguridad en línea en el país—, inicialmente enfocado en la protección de NNA frente al ciberacoso y la circulación de material de abuso sexual infantil, cuyo mandato fue posteriormente ampliado y consolidado mediante el *Online Safety Act* de 2021[21]. Sobre esta arquitectura regulatoria, en diciembre de 2024 el país adoptó una aproximación distinta y particularmente influyente en el debate reciente, al aprobar una reforma al *Online Safety Act* que obliga a determinadas redes sociales a adoptar medidas razonables para impedir que personas con menos de 16 años mantengan cuentas. La obligación entró en vigor en diciembre de 2025. A diferencia de los modelos centrados principalmente en introducir salvaguardas en el diseño y funcionamiento de los servicios, esta aproximación coloca la edad como condición de acceso, abriendo simultáneamente debates sobre mecanismos para determinar la edad de las personas usuarias, privacidad, autonomía progresiva y acceso a información.

Estos modelos no permanecieron circunscritos a las jurisdicciones donde surgieron. Como ha pasado en otros ámbitos de la regulación en temas digitales, sus conceptos e instrumentos pasaron a influir en discusiones de otros países y regiones, incluida América Latina.

21 Disponible en: https://www.legislation.gov.au/C2021A00076/latest/text



02

TENDENCIAS LEGISLATIVAS EN AMÉRICA LATINA PARA LA PROTECCIÓN Y PROMOCIÓN DE DERECHOS DE NNA EN ENTORNOS DIGITALES

02

02. TENDENCIAS LEGISLATIVAS EN AMÉRICA LATINA PARA LA PROTECCIÓN Y PROMOCIÓN DE DERECHOS DE NNA EN ENTORNOS DIGITALES

En los últimos años, la protección de NNA en entornos digitales ganó relevancia en el debate público y en las agendas legislativas de distintos países de América Latina. El siguiente mapeo presenta las leyes aprobadas y algunos de los principales proyectos de ley discutidos en la región entre junio de 2024 y septiembre de 2026. Se seleccionó este período de poco más de dos años para examinar la evolución reciente de las agendas legislativas sobre protección de NNA en entornos digitales en la región. Durante esta ventana temporal, confluyeron la adopción de restricciones de edad para el uso de redes sociales en Australia, la proliferación de proyectos similares en América Latina y la discusión y aprobación de leyes de alcance más amplio de regulación de servicios digitales para protección de NNA en la región.

El análisis está organizado por país y comprende Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, México, Panamá, Paraguay, Perú y Uruguay. Estos países fueron seleccionados por la relevancia de las iniciativas identificadas durante el período y por permitir observar una diversidad de abordajes regulatorios para la protección de NNA en entornos digitales. La inclusión de los países indicados en el mapeo no implica cualquier tipo de valoración sobre su grado de desarrollo en materia de políticas digitales o de marcos de protección de infancias.

Las iniciativas fueron identificadas mediante búsquedas en los sitios oficiales de los gobiernos y órganos legislativos de los países de la región, complementadas con la revisión de noticias y publicaciones de organizaciones de la sociedad civil.

El mapeo incluye, por un lado, nuevas leyes y reglamentaciones aprobadas durante el período, con particular destaque para Bolivia, Brasil, Colombia, Panamá, Perú y Uruguay, donde fueron adoptados marcos dirigidos a distintos aspectos de la protección de NNA en entornos digitales. Por otro lado, se examinan proyectos de ley que todavía se encontraban en discusión al cierre del período analizado, pero que resultan relevantes tanto por su alcance como por los modelos regulatorios que proponen. En la mayoría de los países, de hecho, buena parte de la actividad legislativa identificada todavía se encontraba en esta segunda etapa.

Es importante señalar que el objetivo de este informe no es realizar un inventario exhaustivo de todas las iniciativas presentadas en estos países, pero identificar casos que permitan observar los distintos modelos regulatorios que vienen siendo adoptados o debatidos. Por esta razón, se priorizaron iniciativas de alcance nacional directamente relacionadas con la protección de NNA en entornos digitales.

Esta delimitación implica dejar fuera del mapeo algunas iniciativas que también forman parte del debate más amplio sobre infancias y tecnologías, pero cuyo objeto principal no es la regulación de los entornos digitales. En particular, no se incluyen las normas y proyectos centrados específicamente en restringir o regular el uso de teléfonos celulares y otros dispositivos en establecimientos educativos. Aunque estas medidas han adquirido una presencia importante en las agendas legislativas de distintos países de la región y pueden responder a preocupaciones relacionadas con el bienestar digital de NNA, plantean debates específicos sobre políticas educativas y uso de dispositivos que exceden el objeto de este informe. Tampoco incluye marcos normativos más amplios que eventualmente puedan contener dispositivos específicos sobre la protección de NNA, como leyes de protección de datos o la regulación de la inteligencia artificial.

2.1. Argentina

El principal marco de protección de infancias en Argentina es la Ley 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes[22], de 2005. El país cuenta además con legislación específica sobre algunas formas de violencia facilitadas por tecnologías, como el *grooming*. Sin embargo, no ha adoptado un marco legislativo nacional específicamente dirigido a regular de manera integral los derechos y la protección de NNA en entornos digitales. Este ha sido el objetivo de distintos proyectos orientados específicamente a esta materia presentados en 2026. Entre las iniciativas de mayor alcance se encuentra el Proyecto de Ley 2.733-D-2026, Ley de Cuidado y Bienestar Digital - Uso Responsable de Dispositivos y Redes Sociales para Niñas, Niños y Adolescentes[23], presentado en junio. La propuesta busca establecer un marco general para el uso de plataformas de redes sociales y servicios análogos, basado, entre otros principios, en el interés superior, la autonomía progresiva, la privacidad y protección de datos personales, el diseño seguro y la protección por defecto y una responsabilidad reforzada de los proveedores de servicios digitales.

El proyecto establece obligaciones amplias para las plataformas y otros proveedores de servicios digitales. Entre ellas se encuentran deberes de prevención, mitigación y

22 Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/110000-114999/110778/norma.htm

23 Disponible en: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=292460

reparación frente a riesgos previsibles para NNA, así como restricciones a mecanismos de diseño y perfilamiento orientados a maximizar el tiempo de permanencia o explotar vulnerabilidades. La propuesta prohíbe la publicidad comportamental dirigida a NNA con menos de 16 años y establece condiciones específicas para la publicidad dirigida a adolescentes de 16 y 17 años. También identifica como factores de riesgo determinadas características del diseño de los servicios, como patrones oscuros, reproducción automática, notificaciones intrusivas, sistemas de recomendación orientados a maximizar la permanencia e interacciones irrestrictas con terceros.

En materia de acceso a redes sociales, el proyecto establece un sistema escalonado según la edad. Aunque no define qué se entiende por "redes sociales", la propuesta menciona expresamente plataformas como X, Instagram, Facebook, YouTube y TikTok, además de "otros servicios similares". De acuerdo con el texto, las plataformas no podrían permitir la creación o mantenimiento de cuentas por personas con menos de 14 años, incluso con autorización parental. Entre los 14 y 16 años, el acceso requeriría autorización parental. Para hacer efectivas estas restricciones, la propuesta exige sistemas técnicos de determinación de edad, excluyendo la autodeclaración como único mecanismo. El proyecto prevé además un mecanismo estatal de comprobación que comunicaría a las plataformas únicamente si la persona supera o no el umbral de edad aplicable, sin transferir datos como número de documento, domicilio, imagen biométrica o fecha exacta de nacimiento.

Junto a esta propuesta más amplia, durante 2026 fueron presentadas otras iniciativas concentradas particularmente en las condiciones de acceso a redes sociales. El Proyecto de Ley 1.114-D-2026[24], presentado en abril, propone crear un régimen de protección, uso responsable y acompañamiento parental. La iniciativa establece también un sistema escalonado según la edad, aunque con umbrales diferentes, prohibiendo la creación de cuentas por personas con menos de 13 años, salvo excepciones limitadas basadas en su interés superior; entre los 14 y 16 años, condicionando el acceso al consentimiento parental; y entre los 16 y 18 años permitiendo la creación y utilización de cuentas, salvo que exista una restricción judicial. La propuesta establece además obligaciones para los proveedores de servicios digitales, incluyendo la implementación de sistemas de determinación de edad y mecanismos para comprobar el consentimiento parental cuando corresponda.

En septiembre de 2026 se presentó además el Proyecto de Ley 4.477-D-2026[25], que propone establecer una "mayoría digital" a los 15 años para el acceso a redes sociales. Las personas con menos de 15 años requerirían autorización de sus responsables para

24 Disponible en: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=290679

25 Disponible en: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=294254

acceder a estos servicios. La propuesta también incorpora obligaciones para las plataformas, incluyendo mecanismos de determinación de edad y consentimiento parental, configuraciones de máxima privacidad y seguridad por defecto, desactivación de la geolocalización y limitaciones al perfilamiento con fines publicitarios y a determinados sistemas de recomendación. Los datos utilizados para verificar la edad o la autorización parental no podrían utilizarse para finalidades diferentes.

La actualización de la respuesta penal frente a formas de violencia facilitadas por tecnologías también formó parte del debate legislativo reciente. En abril de 2026, por ejemplo, se presentó el Proyecto de Ley 1.241-D-2026[26], que propone modificar el artículo 131 del Código Penal, relativo al *grooming*. La iniciativa busca actualizar el tipo penal aplicable al contacto con NNA mediante comunicaciones electrónicas, telecomunicaciones u otras tecnologías de transmisión de datos con fines sexuales. En junio además se presentó el Proyecto de Ley 2.744-D-2026[27], que propone modificar el Código Penal para incorporar expresamente el uso de técnicas de inteligencia artificial en la generación y difusión de imágenes de contenido sexual, ampliando la respuesta penal frente a nuevas formas de producción de material sexual que involucre o represente a NNA.

2.2. Bolivia

Bolivia tiene desde 2014 un marco de protección integral de la infancia y adolescencia denominado Código Niña, Niño y Adolescente (Ley 548 de 2014)[28]. A este se sumó, en septiembre de 2025, la Ley 1.636 para la Protección de la Integridad Sexual de Niñas, Niños y Adolescentes en Entornos Digitales[29], el principal cambio legislativo del país en esta materia durante el período analizado. La norma tiene como objeto identificar, investigar y sancionar delitos contra la integridad sexual de NNA cometidos mediante tecnologías de la información y la comunicación y se presenta como la primera norma boliviana específicamente dirigida a la violencia sexual contra NNA en entornos digitales.

La Ley 1.636 mantiene una orientación fuertemente vinculada al derecho penal y a la persecución de delitos. Entre otros cambios, modifica el Código Penal para incorporar o actualizar conductas relacionadas con violencia sexual en entornos digitales y establece instrumentos destinados a facilitar su investigación. De acuerdo con

26 Disponible en: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=290893

27 Disponible en: https://www.hcdn.gob.ar/proyectos/detalle_tp_adjunto/index.html?id=292465

28 Disponible en: https://www.coordinadoradelamujer.org.bo/observatorio/archivos/marco/l548_389.pdf

29 Disponible en: https://www.lexivox.org/norms/BO-L-N1636.xhtml

la Fiscalía General del Estado, la legislación buscó responder a dificultades para investigar y sancionar fenómenos como *grooming*, sextorsión y producción y circulación de material de abuso sexual infantil[30].

La norma, sin embargo, también contempla mecanismos de prevención, protección, reparación y rehabilitación de las víctimas y determina que el Ministerio de Salud y Deportes implemente planes, programas y servicios especializados de salud mental para NNA víctimas de delitos en entornos digitales. Entre ellas, la Ley 1.636 obliga a estas empresas a proporcionar a las autoridades competentes, en un plazo de 24 horas, la información y documentación requerida para la investigación de los delitos previstos por la ley y a conservar durante al menos dos años datos y metadatos derivados de las comunicaciones, incluyendo direcciones IP, origen geográfico, frecuencia y datos de navegación.

Asimismo, establece responsabilidades específicas para empresas públicas y privadas que prestan servicios de telecomunicaciones y tecnologías de la información y comunicación, como la prohibición de difusión de datos personales o imágenes de víctimas y la eliminación inmediata de contenido sexual infantil de plataformas digitales.

2.3. Brasil

Brasil cuenta desde 1990 con el Estatuto da Criança e do Adolescente (ECA)[31] como marco general para la protección de NNA. Durante el período analizado, adoptó la Ley 15.211 (ECA Digital), de septiembre de 2025[32], que establece reglas para la protección de NNA en entornos digitales y se aplica a productos y servicios de tecnología de la información dirigidos a este público o de acceso probable por él, independientemente del lugar donde se encuentren las empresas responsables de su desarrollo, oferta u operación.

La norma aborda diferentes dimensiones de la relación entre NNA y servicios digitales. Establece obligaciones de prevención y mitigación de riesgos relacionados, entre otros, con explotación y abuso sexual, violencia y ciberacoso, autolesiones y suicidio, juegos de azar, prácticas comerciales perjudiciales y contenido pornográfico. Asimismo, la ley incorpora una lógica de protección por diseño, lo que significa que productos y servicios dirigidos a NNA o de acceso probable por ellos deben adoptar por defecto la configuración más protectora disponible en materia de privacidad y protección de datos personales. El marco también establece requisitos para herramientas de supervisión parental, productos de mo-

30 Disponible en: https://www.fiscalia.gob.bo/fiscalias-superiores/fiscalia-superior-en-razon-de-genero/ley-n1636

31 Disponible en: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm

32 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

nitoreo infantil y funcionalidades de interacción en juegos electrónicos.

Con relación al acceso a redes sociales, la ley exige que las cuentas de NNA de hasta 16 años estén vinculadas a la cuenta de una persona responsable legal. Por otro lado, se prohíbe la creación de perfiles de NNA para fines de publicidad comercial. Del mismo modo, se prohíbe el uso de determinadas tecnologías, entre ellas análisis emocional, realidad aumentada, extendida o virtual, para esta finalidad.

Finalmente, la norma establece obligaciones de remoción y comunicación a las autoridades competentes sobre contenidos relacionados con explotación o abuso sexual, secuestro y *grooming*. La ley atribuye a la Agencia Nacional de Protección de Datos (ANPD) las funciones de reglamentación y fiscalización.

Según el Decreto 12.880/2026[33], que reglamenta el ECA Digital e instituye la Política Nacional de Promoción y Protección de los Derechos de Niñas, Niños y Adolescentes en el Ambiente Digital, principios como proporcionalidad, necesidad, seguridad, privacidad y protección de datos personales deben ser observados en los mecanismos de averiguación de edad. El decreto desarrolla las disposiciones de la ley relativas a temas como el diseño adictivo y reglamenta la participación de NNA como creadores de contenido digital con fines comerciales, estableciendo la exigencia de autorización judicial previa para la monetización o el impulso remunerado de contenidos en redes sociales y otras plataformas digitales.

Pese a la aprobación del ECA Digital y la publicación de su decreto reglamentario, siguen en trámite proyectos como el Projeto de Lei 2.387/2025[34] y las iniciativas anexadas a él, que proponen prohibir el acceso a redes sociales a menores de 16 años, una restricción más amplia que la presente en la ley vigente.

Otra vertiente de la regulación brasileña durante el período se concentró en un enfoque penal contra la violencia sexual facilitada por tecnologías digitales. En agosto de 2026 fue aprobada la Ley 15.487/2026[35], que modificó el Estatuto da Criança e do Adolescente (ECA), el Código Penal, el Código de Proceso Penal y otras normas para ampliar y endurecer el tratamiento penal de diferentes conductas relacionadas con violencia sexual contra NNA, incluyendo aquellas practicadas en entornos digitales y mediante inteligencia artificial.

33 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

34 Disponible en: https://www.camara.leg.br/proposicoesWeb/prop_visual_impress?idProposicao=2511795&ord=1

35 Disponible en: https://planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

La norma abarca la producción, transmisión, almacenamiento y acceso a material de violencia sexual e incluye expresamente representaciones producidas, manipuladas o generadas mediante inteligencia artificial, *deepfakes* y otros recursos de alteración de imágenes o voces. También prevé un aumento de pena de un tercio a dos tercios cuando los delitos se cometen mediante técnicas de enmascaramiento, ocultación, falsificación, alteración o anonimización de direcciones IP u otros identificadores digitales, entre las que podría incluirse el uso de redes privadas virtuales (VPN). Asimismo, reconoce el derecho de NNA víctimas o testigos de violencia sexual a recibir atención psicológica y psicosocial individual, especializada, continua e integral.

2.4. Chile

Chile cuenta con un marco general de protección de los derechos de NNA establecido por la Ley 21.430 sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia[36], de 2022, que reconoce expresamente derechos relacionados con la vida privada, la protección de datos personales y el acceso a información y tecnologías. Durante el período analizado, un número creciente de proyectos dirigidos específicamente a la protección de NNA en entornos digitales fue presentado buscando complementar el marco general existente.

En junio de 2025 fue presentado el Boletín 17.624-19[37], que propone regular el contenido que las plataformas de servicios digitales ofrecen a NNA y prevenir su adicción a las redes sociales. La propuesta parte de los riesgos de determinadas características de las plataformas sobre el bienestar de NNA y plantea obligaciones dirigidas a reducir su exposición a contenidos y dinámicas consideradas perjudiciales.

Durante 2026, este debate se amplió considerablemente. En abril se presentó el Boletín 18.224-18[38], que propone establecer un marco integral de protección de NNA en el uso de redes sociales. En los meses siguientes, esta iniciativa fue refundida con otros proyectos que abordan, desde distintas perspectivas, la protección frente al uso adictivo de tecnologías, la responsabilidad algorítmica y la protección digital de NNA y la incorporación de principios de protección de la infancia en el marco de ciberseguridad.

36 Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1173643

37 Disponible en: https://www.camara.cl/verDoc.aspx?prmID=17852&prmTIPO=INICIATIVA

38 Disponible en: https://www.camara.cl/verDoc.aspx?prmID=36328&prmTipo=DOCUMENTO_COMISIONDOCUMENTO

Entre los proyectos refundidos destaca el Boletín 18.318-19[39], que propone un estatuto de responsabilidad algorítmica y protección digital de NNA. La iniciativa contempla la regulación del acceso a plataformas conforme a la autonomía progresiva, la prohibición del diseño algorítmico adictivo y de patrones oscuros dirigidos a NNA, restricciones a la publicidad comportamental y al perfilamiento algorítmico, estándares reforzados de protección de datos personales y un régimen específico de responsabilidad para los proveedores de plataformas digitales.

La determinación de edad también ocupa un lugar central en estas propuestas. El Boletín 18.224-18[40] exige que los operadores implementen mecanismos técnicamente viables y proporcionales al nivel de riesgo del servicio, compatibles con la privacidad y la protección de datos personales. El proyecto prevé impedir el acceso de personas con menos de 14 años sin consentimiento verificable de sus responsables y exigir mecanismos de confirmación de edad para adolescentes de entre 14 y 17 años. También establece que los datos utilizados para este propósito no puedan ser reutilizados para publicidad, perfilamiento comercial, personalización de contenidos u otras finalidades ajenas a la determinación.

Paralelamente, adquirieron fuerza propuestas que plantean restricciones de acceso según la edad aún más amplias. En enero de 2026 se presentó el Boletín 18.090-19[41], que, "con el propósito de proteger el bienestar físico, psicológico, social y moral de los niños, niñas y adolescentes", propone prohibir el acceso a plataformas de redes sociales a personas con menos de 16 años y establecer exigencias específicas para sus proveedores. Durante los meses siguientes se presentaron otras iniciativas con diferentes umbrales y mecanismos.

Otra vertiente corresponde a la incorporación de la protección de NNA directamente en el marco general de derechos de la infancia. El Boletín 18.320-18[42], presentado en junio de 2026, propone modificar la Ley 21.430 para incorporar medidas específicas de protección de la infancia y adolescencia en entornos digitales. La iniciativa parte del marco de protección integral ya existente y busca complementarlo frente a riesgos derivados del uso de internet, redes sociales y otras tecnologías digitales.

39 Disponible en: https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=85850

40 Disponible en: https://www.camara.cl/verDoc.aspx?prmID=36328&prmTipo=DOCUMENTO_COMISIONDOCUMENTO

41 Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/81963/4/20260303_97_18090-19.pdf

42 Disponible en: https://camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=18993&prmBOLETIN=18320-18

La actualización de la respuesta penal frente a formas de violencia facilitadas por tecnologías también forma parte del escenario legislativo chileno. En mayo de 2025 se presentó el Boletín 17.534-07[43], que propone modificar el Código Penal para ampliar las hipótesis del delito de *grooming*. La iniciativa busca extender el alcance del tipo penal frente a interacciones sexuales mantenidas con NNA a través de medios tecnológicos.

2.5. Colombia

Colombia cuenta con el Código de la Infancia y la Adolescencia, aprobado mediante la Ley 1.098 de 2006[44], como marco general para la protección de NNA. Durante el período analizado, el país adoptó una serie de medidas legislativas relacionadas con la protección de NNA en entornos digitales.

En julio de 2025 fue aprobada la Ley 2.489 de 2025[45], que establece disposiciones para el desarrollo de entornos digitales sanos y seguros para NNA. Su objeto es promover una política pública que articule acciones del Estado, las familias, las empresas, las organizaciones sin fines de lucro y la sociedad civil para prevenir riesgos en línea, promover hábitos saludables en el uso de tecnologías y garantizar los derechos de NNA. Aunque la ley parte de un principio de corresponsabilidad entre diferentes actores, sus disposiciones se concentran principalmente en obligaciones a cargo del Estado. Entre ellas se encuentran la formulación de políticas de prevención, educación y sensibilización, la promoción de competencias digitales y la creación de mecanismos de monitoreo y evaluación.

El marco fue posteriormente reglamentado por el Decreto 769 de 2026[46], que avanzó en la definición de responsabilidades de los actores privados que intervienen en la configuración de los entornos digitales. El decreto alcanza, entre otros, a proveedores de redes y servicios de telecomunicaciones, plataformas y servicios digitales, aplicaciones, videojuegos y sistemas de inteligencia artificial accesibles a NNA en Colombia. Entre sus disposiciones se incluyen estándares de seguridad y privacidad desde el diseño y por defecto, así como medidas de debida diligencia y gestión de riesgos asociados a los servicios digitales.

43 Disponible en: https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmID=18174&prmBOLETIN=17534-07

44 Disponible en: https://www.icbf.gov.co/sites/default/files/codigoinfancialey1098.pdf

45 Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=260756

46 Disponible en: https://www.arielapp.co/es/biblioteca/documento/decreto-769-de-2026-cc36e219

En enero de 2026 también fue sancionada la Ley 2.564[47], orientada específicamente a la salud mental y a distintas formas de violencia en el entorno digital. La norma establece medidas de sensibilización, prevención, protección y atención e identifica manifestaciones de violencia digital como *grooming*, sextorsión, *stalking,* ciberacoso, *cyberbullying y happy slapping.* Su tramitación estuvo marcada por el lobby de grandes empresas tecnológicas y de asociaciones que representan sus intereses, dirigida a limitar las obligaciones y responsabilidades que el proyecto imponía a las plataformas digitales[48]. Como resultado, disposiciones que buscaban regular contenidos potencialmente nocivos para la salud mental de NNA fueron modificadas durante el trámite legislativo, y el texto finalmente aprobado no establece obligaciones sustantivas para las proveedoras de servicios.

Durante el período analizado también se presentaron distintas iniciativas que no han sido convertidas en ley. Entre ellas está el Proyecto de Ley 3.06/2025C[49], que propone establecer medidas para prevenir, tipificar y sancionar el *grooming* o los acercamientos sexuales digitales abusivos contra NNA. La iniciativa busca incorporar una respuesta penal específica a estas conductas y complementarla con medidas de prevención y educación.

También en 2025 fue presentado el Proyecto de Ley 394/2025C[50], que propone regular la actividad de creadores de contenido digital y, en ese tema, también establecer disposiciones específicas para la protección de los derechos de NNA. La iniciativa contempla obligaciones para plataformas digitales y otros intermediarios relacionados, entre otros aspectos, con la identificación, moderación y retiro de determinados contenidos y con la protección de NNA que participan en la creación de contenido.

Finalmente, las restricciones etarias para el acceso a redes sociales también ganaron espacio en el Congreso colombiano. En agosto de 2026, fue radicado el proyecto de ley estatutaria "Niños Sin Redes" (208/2026C)[51], que propone establecer el límite

47 Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%20No.%202564%20DEL%208%20DE%20ENERO%20DE%202026.pdf

48 Olga Lucia Camacho, "El lobby de las Big Tech frena la regulación en Colombia", *La Silla Vacía* (19 de mayo de 2026), disponible en: https://www.lasillavacia.com/red-de-expertos/red-de-democracia-y-tecnologia/el-lobby-de-las-big-tech-frena-la-regulacion-en-colombia/

49 Disponible en: https://www.camara.gov.co/ley-contra-el-grooming-067/

50 Disponible en: https://leyes.senado.gov.co/p-ley/2024-2025/PL%20394-25%20CONTENIDO%20DIGITAL.pdf

51 Disponible en: https://www.camara.gov.co/ninos-sin-redes/

etario de 16 años para la creación y mantenimiento de cuentas en redes sociales, mecanismos de determinación de edad y obligaciones de seguridad y diseño responsable para los proveedores.

2.6. Ecuador

Ecuador cuenta desde 2003 con el Código de la Niñez y Adolescencia (Ley 100)[52], que establece un marco general de protección integral y garantía de los derechos de NNA en el país. En el periodo analizado, diferentes iniciativas legislativas sobre el tema fueron discutidas, abarcando temas como la regulación de redes sociales y de la inteligencia artificial, la explotación sexual facilitada por tecnologías y la exposición económica de NNA en plataformas digitales.

Una de estas discusiones se desarrolló en el marco de la construcción de una legislación general sobre inteligencia artificial. El Proyecto de Ley Orgánica de Aprovechamiento Digital e Inteligencia Artificial para Niñas, Niños y Adolescentes[53], presentado en 2024, buscaba garantizar el uso seguro de internet, redes sociales y plataformas digitales por NNA y establecía disposiciones específicas sobre el desarrollo y utilización de sistemas de inteligencia artificial relacionados con este público. La iniciativa fue posteriormente unificada a dos otras propuestas sobre el tema —el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial[54], el Proyecto de Ley para el Fomento y Desarrollo de la Inteligencia Artificial[55]— en una propuesta general de regulación de la IA. El informe para el primer debate fue presentado en septiembre de 2026 y recomendó su archivo, decisión que finalmente fue acogida por el Pleno de la Asamblea Nacional[56].

52 Disponible en: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2017/11/codigo_ninezyadolescencia.pdf

53 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/99931-proyecto-de-ley-organica-de

54 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/97303-proyecto-de-ley-organica-de-regulacion

55 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/98762-proyecto-de-ley-para-el-fomento-y

56 Disponible en: https://www.lexis.com.ec/noticias/pleno-de-la-asamblea-naciona-archiva-proyecto-de-ley-de-inteligencia-artificial-en-primer-debate

Otra línea regulatoria se desarrolló mediante una propuesta de reforma al Código de la Niñez y Adolescencia[57]. La propuesta prohíbe el acceso y uso de redes sociales a NNA con menos de 15 años y establece que las empresas y plataformas tecnológicas privadas que ofrecen estos servicios deben adoptar las medidas necesarias y eficaces para garantizar el cumplimiento de esta restricción, incluido el establecimiento de mecanismos de determinación de edad.

Durante el período también se discutió un Proyecto de Ley Orgánica para el Uso Responsable de Redes Sociales, dirigido tanto a NNA como a la ciudadanía en general. Sin embargo, en junio de 2026, el Pleno de la Asamblea Nacional decidió archivarlo por unanimidad[58]. Entre las razones señaladas por la Comisión legislativa se encontraban posibles restricciones desproporcionadas a la libertad de expresión y al acceso a la información, el carácter excesivamente sancionatorio de la propuesta, vacíos en materia de protección de datos personales y la falta de claridad sobre las instituciones responsables de su fiscalización y sanción. La Comisión consideró, además, que la propuesta no incorporaba adecuadamente la protección reforzada de NNA ni los riesgos específicos asociados al uso de redes sociales.

En relación con la respuesta penal frente a la producción y circulación de material de abuso sexual infantil, durante 2026 fueron presentadas dos iniciativas legislativas. En marzo, la Ley Orgánica Reformatoria al Código Orgánico Integral Penal para la Tipificación de Conductas Vinculadas a la Explotación Sexual de Niñas, Niños y Adolescentes mediante Inteligencia Artificial y otras Tecnologías de la Información[59], que propuso sancionar la creación, simulación, difusión y utilización de material de carácter sexual generado o manipulado mediante IA u otras tecnologías, con penas de hasta trece años.

En abril se presentó una segunda iniciativa, posteriormente denominada Proyecto de Ley Orgánica para la Prevención, Erradicación y Sanción Frente a los Delitos Vinculados con Material de Abuso Sexual Infantil (Ley de Infancia Segura)[60], con un alcance más amplio,

57 Disponible en: https://www.asambleanacional.gob.ec/es/node/111803

58 Disponible en: https://www.asambleanacional.gob.ec/es/noticia/117423-pleno-archiva-el-proyecto-de-ley-para-el-uso

59 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/115385-proyecto-de-ley-organica-reformatoria

60 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/116939-proyecto-de-ley-organica-para-la

que combina medidas de prevención y protección con reformas penales y a la legislación de telecomunicaciones. Durante su tramitación se abordaron, entre otras cuestiones, el uso de inteligencia artificial para la creación de material de abuso sexual infantil, las obligaciones de proveedores de servicios de internet y mecanismos de bloqueo de contenidos.

Finalmente, en otra materia, en julio de 2026 se presentó el Proyecto de Ley Orgánica de Protección Integral de Niñas, Niños y Adolescentes en Entornos Digitales y de Exposición Económica[61], que aborda la monetización de la imagen y actividad de NNA en plataformas digitales. Su ámbito comprende actividades en las que su imagen, voz, identidad, talento o presencia pública sean utilizados para generar ingresos o beneficios económicos y propone salvaguardas patrimoniales, mecanismos de debida diligencia y responsabilidades administrativas frente a situaciones de explotación económica y sobreexposición.

2.7. México

México cuenta con un marco general de protección de los derechos de NNA establecido por la Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA)[62], de 2014, que contiene disposiciones relacionadas con el acceso y uso seguro de internet, la privacidad y la protección de datos personales. Durante el período analizado se presentaron distintas iniciativas para ampliar este marco frente a los riesgos asociados a redes sociales y nuevas formas de violencia facilitada por tecnologías.

Una de las propuestas de mayor alcance fue presentada en el Senado el 18 de febrero de 2025[63]. La iniciativa busca reformar la LGDNNA y la Ley Federal de Telecomunicaciones y Radiodifusión para impedir el acceso a redes sociales a personas con menos de 14 años y exigir consentimiento de madres, padres o responsables para el registro de adolescentes de entre 14 y 17 años. Exige además mecanismos de determinación de edad y control parental, establece configuraciones de máxima privacidad por defecto para las cuentas de adolescentes y considera sus datos personales como sensibles. También atribuye a las plataformas responsabilidades para implementar medidas de seguridad, impedir activamente el acceso a servicios inadecuados y establecer

61 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/118717-proyecto-de-ley-organica-de-proteccion

62 Disponible en: https://www.gob.mx/cms/uploads/attachment/file/918955/LGDNNA_Ultima_Reforma__27052024.pdf

63 Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la Ley General de los Derechos de Niñas, Niños y Adolescentes y de la Ley Federal de Telecomunicaciones y Radiodifusión. Disponible en: https://www.senado.gob.mx/66/gaceta_del_senado/2025_02_18/3562

mecanismos de denuncia y reparación.

El 9 de septiembre de 2025, otro proyecto fue presentado buscando incorporar a la LGDNNA el derecho de NNA a un entorno digital seguro mediante la adición de una fracción XXI al artículo 13[64]. La iniciativa reconoce el derecho a participar y desarrollarse en espacios digitales protegidos frente a la violencia, explotación, acoso, manipulación, extorsión, exposición a contenidos inapropiados y vulneraciones de la privacidad, y dispone que las autoridades competentes promuevan medidas de prevención, protección y orientación digital.

Aquel mismo mes, otra iniciativa fue presentada proponiendo reformar los artículos 66 y 76 de la LGDNNA[65], con énfasis en los riesgos derivados del acceso y uso de tecnologías, redes sociales y sistemas de información y en la protección de la privacidad y de los datos personales. La exposición de motivos desarrolla además la necesidad de establecer responsabilidades para las plataformas, incluyendo mecanismos de determinación de edad, configuraciones de máxima privacidad por defecto y herramientas de moderación de contenidos.

En temas de ciberseguridad y violencia facilitada por las tecnologías, un proyecto de ley de marzo de 2026 propone incorporar a la LGDNNA un capítulo sobre el derecho a la seguridad y protección en el entorno digital[66]. Entre sus disposiciones, la iniciativa establece obligaciones estatales de prevención del ciberacoso, *grooming* y explotación sexual digital; prevé mecanismos de alerta y denuncia y cooperación con plataformas para el retiro de contenidos que vulneren sus derechos; y prohíbe expresamente la creación o difusión de contenidos manipulados digitalmente que simulen imágenes íntimas de NNA mediante inteligencia artificial.

64 Iniciativa que adiciona la fracción XXI del artículo 13 de la Ley General de los Derechos de Niñas, Niños y Adolescentes, en materia de un entorno digital seguro. Disponible en: https://gaceta.diputados.gob.mx/PDF/66/2025/sep/20250909-II-1-1.pdf

65 Iniciativa que reforma diversas disposiciones de la Ley General de los Derechos de Niñas, Niños y Adolescentes. Disponible en: https://gaceta.diputados.gob.mx/PDF/66/2025/sep/20250923-II-1.pdf

66 Iniciativa que adiciona diversas disposiciones de la Ley General de los Derechos de Niñas, Niños y Adolescentes, en materia de ciberseguridad y protección digital. Disponible en: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-6.pdf

En marzo de 2026, se presentó también una iniciativa para tipificar el grooming en el Código Penal Federal bajo la denominación de "inducción sexual mediante engaño digital"[67]. La propuesta sanciona el establecimiento de un vínculo de confianza con una persona menor de 18 años a través de medios digitales para inducirla a generar contenido sexual íntimo o concretar un encuentro sexual, aunque estos fines no lleguen a materializarse. Prevé aumentos de pena cuando se emplean inteligencia artificial generativa, automatización, identidades o perfiles falsos o tecnologías para modificar la apariencia o la voz. También establece medidas preventivas para los servicios digitales, como seguridad por diseño, controles parentales activados por defecto y canales prioritarios de denuncia y bloqueo.

2.8. Panamá

Panamá cuenta con un marco general de protección de NNA establecido por la Ley 285 de 2022, que crea el Sistema de Garantías y Protección Integral de los Derechos de la Niñez y la Adolescencia[68]. En el período analizado, el país avanzó en la actualización de su legislación penal frente a la violencia facilitada por tecnologías por medio de la Ley 478 de 4 de agosto de 2025[69], que modifica y adiciona disposiciones al Código Penal, al Código Procesal Penal y a la legislación sobre asistencia jurídica internacional en materia penal.

En lo referente a la protección de NNA, la ley sanciona la producción, comercialización, difusión y distribución de material de abuso sexual infantil que represente a personas con menos de 18 años en actividades sexuales reales o simuladas, así como la posesión para uso propio de material adquirido voluntariamente. También tipifica el contacto con NNA con fines de cometer delitos contra su libertad e integridad sexual, incluso por medios digitales. La reforma incorpora además medidas de investigación penal relativas al registro, incautación, conservación y suministro de datos informáticos.

67 Iniciativa que reforma y adiciona diversas disposiciones del Código Penal Federal, de la Ley General de Educación y de la Ley General de los Derechos de Niñas, Niños y Adolescentes, en materia de protección digital e inducción sexual mediante engaño. Disponible en: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-3.pdf

68 Disponible en: https://www.defensoria.gob.pa/wp-content/uploads/LEY-285-SISTEMA-DE-GARANTIAS-Y-PROTECCION-INTEGRAL-DE-LOS-DERECHOS-DE-LA-NINEZ-Y-LA-ADOLESCENCIA.pdf

69 Disponible en: https://igc-panama.org/wp-content/uploads/2025/08/Ley-478.-Ciberdelincuencia.pdf

En cuanto a la discusión legislativa, el Proyecto de Ley 426[70] busca regular los servicios en línea y redes sociales para la protección digital de los NNA. La propuesta es una de las principales en debate sobre el tema y tuvo origen en los mecanismos de participación ciudadana de la Asamblea Nacional, siendo posteriormente acogida para tramitación legislativa[71]. El proyecto establece reglas específicas para el acceso de NNA a redes sociales, incluyendo la prohibición del acceso a personas con menos de 14 años. Además, establece obligaciones para que los proveedores implementen mecanismos de determinación de edad y herramientas de control parental. La propuesta contempla además medidas destinadas a reducir la exposición a contenidos perjudiciales y establece responsabilidades para los proveedores respecto de la seguridad de NNA en sus servicios.

La iniciativa incorpora asimismo deberes de transparencia y rendición de cuentas a los proveedores de servicios en línea y redes sociales que ofrezcan servicios a personas en Panamá, así como obligaciones de colaboración con las autoridades competentes frente a posibles delitos cometidos a través de sus servicios. De esta manera, el proyecto combina restricciones de acceso basadas en la edad con obligaciones dirigidas a las propias empresas proveedoras de servicios en línea.

2.9. Paraguay

Paraguay cuenta con un marco general de protección de NNA establecido por la Ley 1.680/2001, Código de la Niñez y la Adolescencia[72]. Durante el período analizado, el país aprobó la Ley 7.549/2025[73], que dispone la obligatoriedad de la conservación de datos para combatir la diseminación de contenidos de abuso sexual infantil. La norma obliga a todos los proveedores que operan en el país bajo la legislación de telecomunicaciones a conservar durante un período mínimo de 12 meses datos de tráfico como dirección IP, fecha y hora de conexión y desconexión y datos de localización, con la finalidad de permitir la identificación de personas investigadas por estos delitos. Por otro lado, excluye expresamente el contenido de las comunicaciones y establece que el acceso a los datos conservados solamente puede ser solicitado por el Ministerio Público mediante orden judicial en el marco de las investigaciones penales comprendidas por la norma.

70 Disponible en: https://sistemas.asamblea.gob.pa/segLegis/viewsPublico/SeguimientoLegislativo

71 "Estudiantes de Derecho de la USMA promueven proyecto de ley sobre protección digital de menores", *Haciendo Universidad*. 11 de marzo de 2026. Disponible en:https://info.usma.ac.pa/estudiantes-de-derecho-de-la-usma-promueven-proyecto-de-ley-sobre-proteccion-digital-de-menores/

72 Disponible en: https://www.bacn.gov.py/leyes-paraguayas/5261/codigo-de-la-ninez-y-laadolescencia

73 Disponible en: https://silpy.congreso.gov.py/web/descarga/ley-146014?preview

Durante 2026 adquirió mayor presencia en Paraguay el debate sobre marcos más amplios de protección de NNA en entornos digitales y restricciones de acceso a redes sociales. Estas discusiones tienen como antecedente la Ley 5.653/2016, de Protección de Niños, Niñas y Adolescentes contra Contenidos Nocivos de Internet[74], reglamentada por el Decreto 8.098/22[75], que obliga a los proveedores de servicios de internet a suministrar de manera obligatoria y gratuita un software con sistemas de bloqueo de contenidos. Además, crea el Observatorio Nacional para la Protección de los Derechos del Niño, Niña y el Adolescente en Internet que tiene entre sus funciones "planificar, presentar y ejecutar el plan anual para la protección y promoción de los derechos de niños, niñas y adolescentes en internet".

En marzo de 2026, el Senado anunció una audiencia pública sobre un proyecto que modifica y amplía la Ley 5.653/2016 para incluir entre las obligaciones de los proveedores la oferta de herramientas de control parental y seguridad digital que puedan operar a nivel de red o de los sistemas operativos. También contempla medidas para prevenir el acceso de NNA a plataformas, servicios o funcionalidades que promuevan patrones de uso intensivo o potencialmente perjudiciales para su bienestar físico y mental. En el mismo mes, la Comisión de Ciencias, Tecnología, Innovación y Futuro informó que su agenda incluía el análisis de una propuesta para regular o prohibir el uso de redes sociales por personas con menos de 16 años[76].

A las propuestas legislativas en curso, se sumó durante 2026 un proceso impulsado por el Ministerio de la Niñez y la Adolescencia, el Ministerio de Tecnologías de la Información y Comunicación y otros actores para desarrollar un marco de protección de NNA en entornos digitales. Si bien la propuesta todavía no se ha hecho pública, información oficial indica que la propuesta estaría orientada a combinar educación digital, participación de las familias y medidas frente a riesgos asociados a plataformas digitales, ciberdelitos y contenidos generados mediante inteligencia artificial[77].

Desde la perspectiva criminal, en noviembre de 2024 fue presentado el Proyecto de

74 Disponible en: https://baselegal.com.py/docs/4870f1b5-5c8a-11ed-be69-525400343722

75 Disponible en: https://baselegal.com.py/docs/ec914bf2-5c8c-11ed-be69-525400343722

76 Disponible en: https://www.senado.gov.py/index.php/menu-dircom/sub-menu-noticias-generales/analizaran-propuesta-legislativa-sobre-uso-de-redes-sociales-en-menores-2026-03-05-15-48-52.html

77 Disponible en: https://www.ip.gov.py/ip/2026/05/26/paraguay-impulsa-proyecto-de-ley-que-apunta-a-establecer-entornos-digitales-seguros-para-ninos-y-adolescentes/

Ley D-2481664[78] con el objetivo de establecer un marco específico para la prevención, detección, sanción y erradicación del *grooming*.

2.10. Perú

Perú cuenta con el Código de los Niños y Adolescentes, establecido mediante la Ley 27.337 de 2000[79] como marco general de protección de NNA. Además, en 2014 aprobó la Ley 30.254 para la Promoción del Uso Seguro y Responsable de las Tecnologías de la Información y Comunicaciones por Niñas, Niños y Adolescentes[80]. Aún así, el debate sobre la protección de NNA en entornos digitales adquirió un nuevo alcance durante el período analizado.

Una de las principales modificaciones legislativas aprobadas se produjo en el ámbito penal. Se trata de la Ley 32.314[81], de 2025, que modifica el Código Penal, y la Ley 30.096, sobre Delitos Informáticos, que incluye el uso de IA en la comisión de delitos. Entre otras modificaciones, la ley reformó el artículo 129-M del Código Penal, relativo a materiales de abuso sexual infantil, para incluir expresamente a los *deepfakes* y otros contenidos multimedia generados mediante IA.

Otras iniciativas legislativas aún en discusión buscan establecer marcos más amplios de protección. Entre ellas destaca el Proyecto de Ley 10.880/2024-CR[82], que, entre otras medidas, incluía provisiones para limitar el acceso a dispositivos móviles y redes sociales por menores de edad. En el caso de las redes sociales, se prohibía la creación de cuentas propias a menores de 16 años.

La versión inicial del proyecto fue objetivo de críticas debido a la inclusión de medidas de identificación biométrica para verificar la edad, restricciones y obligaciones relacionadas con servicios de VPN y medidas técnicas de control y bloqueo de contenidos. La propuesta fue modificada durante su tramitación. En noviembre de 2025, la Comisión de Mujer y Familia aprobó un texto sustitutorio[83] enfocado en establecer principios

78 Disponible en: https://silpy.congreso.gov.py/web/expediente/138173

79 Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/3366849-27337

80 Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292146-30254

81 Disponible en: https://img.lpderecho.pe/wp-content/uploads/2025/04/Ley-32314-LPDerecho.pdf

82 Disponible en: https://vlex.com.pe/vid/proyecto-ley-n-10880-1076983759

83 Disponible en: https://comunicaciones.congreso.gob.pe/despacho-informa/comision-de-mujer-y-familia-aprueba-proyecto-que-garantiza-entornos-digitales-seguros-para-ninos-y-adolescentes/

como el interés superior, la autonomía progresiva, la corresponsabilidad entre Estado, familias y empresas tecnológicas y la neutralidad tecnológica y de red. También contempla medidas para reducir la exposición a contenidos nocivos y prevenir formas de violencia como ciberacoso, *grooming* y sextorsión.

El proyecto continuó avanzando durante 2026. En febrero, la Comisión de Salud y Población aprobó otro dictamen que acumuló los Proyectos de Ley 8017/2023-CR, 10880/2024-CR y 13453/2025-CR y colocó mayor énfasis en la promoción y prevención de la salud mental de NNA en entornos digitales[84]. El texto adoptó un enfoque preventivo, con responsabilidades para el Estado, instituciones educativas y familias y referencias expresas al interés superior, desarrollo progresivo y enfoque de derechos.

Finalmente, el Proyecto de Ley 00498/2026-2031-CD[85] retomó estas iniciativas como antecedentes, manteniendo la prohibición a la creación de cuentas personales en redes sociales por menores de 16 años. La propuesta exige a los proveedores de servicios medidas razonables y proporcionales de determinación de edad, pero no prescribe la identificación biométrica ni establece obligaciones específicas sobre servicios de VPN como la versión original. Además, limita el uso de los datos obtenidos para la comprobación de edad, determinando su eliminación al concluir el proceso, salvo obligación legal de conservación. Para adolescentes de 16 y 17 años, la ley establece criterios específicos para sus cuentas en redes sociales.

2.11. Uruguay

Uruguay cuenta con el Código de la Niñez y la Adolescencia[86], aprobado en 2004, como marco general para la protección de NNA. Durante el período analizado, el país aprobó modificaciones de su legislación penal aplicable a conductas cometidas en entornos digitales con implicaciones sobre las infancias.

La Ley 20.327 de 2024[87] incorporó nuevos delitos y agravantes al Código Penal, tipificando el "acoso telemático" y estableciendo como circunstancia agravante que la conducta se realice en perjuicio de NNA. También incorporó agravantes específicas

84 Disponible en: https://comunicaciones.congreso.gob.pe/noticias/aprueba-dictamenes-para-proteger-la-salud-mental-infantil-y-uso-seguro-de-internet/

85 Disponible en: https://img.lpderecho.pe/wp-content/uploads/2026/10/PL-00498-2026-2031-CD-LP-Derecho.pdf

86 Disponible en: https://www.impo.com.uy/bases/codigo-ninez-adolescencia/17823-2004

87 Disponible en: https://www.impo.com.uy/bases/leyes-originales/20327-2024

al delito previsto en el artículo 277 bis del Código Penal, relacionado con el contacto mediante tecnologías con NNA con fines sexuales, incluyendo los casos en que se utilice coacción, intimidación o engaño, exista una relación de parentesco o afinidad o el contacto se produzca con una persona con menos de 13 años. La ley también considera agravante del delito de vulneración de datos que la víctima sea NNA.

Aún en la esfera criminal, el Proyecto de Ley sobre divulgación de contenidos sexuales elaborados con IA (Carpeta 691/2025)[88] propone extender el delito de la divulgación no consentida de imágenes o grabaciones íntimas o sexuales a contenidos simulados mediante inteligencia artificial, edición digital u otras tecnologías. Entre otras disposiciones, se establece expresamente que la autorización otorgada por NNA para la difusión de estos materiales carece de validez.

Las restricciones etarias para el acceso a redes sociales también ingresaron en la agenda legislativa durante 2026. En julio fue presentado el Proyecto de Ley sobre uso de redes sociales por personas menores de edad (Carpeta 2979/2026)[89], que propone establecer los 15 años como edad mínima para la creación de cuentas en redes sociales. La iniciativa atribuye a las plataformas la responsabilidad de adoptar mecanismos para impedir la creación de cuentas por personas que no alcancen esa edad y prevé un régimen de fiscalización y sanciones.

Estos proyectos se desarrollan en paralelo a un proceso más amplio de discusión sobre la protección de los derechos de NNA en entornos digitales. Durante 2026, el Parlamento, junto con organismos públicos y otras instituciones, impulsó espacios de discusión y una consulta pública sobre infancia, entornos digitales e inteligencia artificial[90]. El proceso abordó cuestiones como responsabilidades de las plataformas, privacidad y protección de datos, violencia digital, mecanismos de determinación de edad y participación de NNA, con el objetivo de generar insumos para futuras políticas públicas e iniciativas legislativas. Al cierre del período analizado, sin embargo, este proceso todavía no se había traducido en la presentación de un proyecto de ley.

88 Disponible en: https://documentos.diputados.gub.uy/docs/L50/Repartid/R0346.pdf

89 Disponible en: https://propaci.parlamento.gub.uy/sipfront/servlet/com.sipfront.unproyectoley?174431

90 Disponible en: https://www.anep.edu.uy/uruguay-avanza-hacia-ley-proteccion-ninas-ninos-adolescentes-en-entornos-digitales



03

PRINCIPALES TENDENCIAS REGULATORIAS EN LA REGIÓN

03

3. PRINCIPALES TENDENCIAS REGULATORIAS EN LA REGIÓN

El mapeo permite identificar algunas tendencias en las respuestas legislativas que vienen siendo adoptadas o discutidas en América Latina. Estas tendencias no son excluyentes entre sí. Por el contrario, en varios países conviven reformas penales, propuestas de restricciones etarias, obligaciones dirigidas a plataformas y nuevas regulaciones sobre otros temas como las actividades económicas desarrolladas por NNA en entornos digitales. Su análisis conjunto permite observar cuáles son las principales cuestiones que han movilizado la actividad legislativa reciente, así como dónde se están concentrando las respuestas estatales.

3.1. Expansión de la respuesta penal y de la vigilancia

El derecho penal continúa ocupando un lugar central en las respuestas legislativas de la región, especialmente frente a la violencia y explotación sexual facilitadas por tecnologías. Esta no es una tendencia nueva. La criminalización del *grooming* y de conductas relacionadas con material de abuso sexual infantil constituye uno de los antecedentes regionales en materia de protección de NNA. A lo largo de décadas, respuestas penales han planteado tensiones entre la ampliación de poderes de vigilancia estatal y la garantía de derechos en los entornos digitales, como ilustran los debates sobre restricciones al cifrado para facilitar la investigación de delitos. Sin embargo, en el período analizado identificamos una nueva etapa de actualización y expansión de estos marcos.

Entre las normas aprobadas, Brasil adoptó la Ley 15.487/2026[91], ampliando el tratamiento penal de distintas formas de violencia sexual contra NNA; Bolivia adoptó la Ley 1.636/2025[92], que incorporó y actualizó tipos penales vinculados a violencia sexual en entornos digitales y amplió instrumentos de investigación; Panamá aprobó la Ley 478/2025[93], que reformó su legislación para incorporar disposiciones aplicables a formas de violencia sexual digital contra NNA; Paraguay aprobó la Ley 7.549/2025[94], que establece obligaciones de conservación de datos para la investigación de delitos relacionados con material de abuso sexual infantil y hechos punibles conexos; y Uruguay

91 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

92 Disponible en: https://www.lexivox.org/norms/BO-L-N1636.xhtml

93 Disponible en: https://igc-panama.org/wp-content/uploads/2025/08/Ley-478.-Ciberdelincuencia.pdf

94 Disponible en: https://silpy.congreso.gov.py/web/ley/146014

aprobó la Ley 20.327/2024[95], que introdujo nuevos delitos y agravantes para conductas realizadas mediante tecnologías. A estas reformas se suman numerosos proyectos de ley todavía en discusión. La actualización de las respuestas al *grooming* y a la producción, posesión y circulación de material de abuso sexual infantil ocupa un lugar destacado en este conjunto de iniciativas.

Más allá de la popularidad de medidas criminalizantes, la creación de nuevos delitos o el aumento de penas no garantizan, por sí mismas, una mayor capacidad de prevención, investigación o protección de las víctimas. Este límite resulta especialmente relevante en América Latina, donde la aplicación de las normas ya existentes enfrenta problemas de recursos, especialización y capacidad técnica para producir y analizar evidencia digital. Un estudio reciente sobre el caso de Brasil señala que, de acuerdo con profesionales del área, las brechas para la protección de NNA se encuentran primordialmente en la implementación de los marcos existentes e incluyen recursos limitados, falta de claridad sobre las responsabilidades de los distintos actores y una coordinación multisectorial insuficiente[96].

Por otro lado, el análisis muestra que el endurecimiento de la respuesta penal viene acompañado, en varias de las iniciativas analizadas, de una ampliación de las capacidades de vigilancia. La creación de delitos y agravantes se articula con nuevas facultades estatales de acceso a información, técnicas de investigación encubierta y obligaciones de conservación, monitoreo y entrega de datos por parte de los proveedores. Así, el impulso punitivo también puede extender el control sobre las actividades digitales de personas que no están siendo investigadas, con impactos sobre la privacidad y la seguridad de las comunicaciones.

En Bolivia, la Ley 1.636/2025[97] permite recurrir a agentes encubiertos en entornos digitales cuando los medios de prueba sean inexistentes o insuficientes, mediante solicitud fundamentada del Ministerio Público y autorización judicial. En Brasil, la Ley 15.487/2026[98] amplía los delitos que pueden investigarse mediante infiltración policial en internet y habilita el patrullaje automatizado de espacios digitales públicos sin autorización judicial previa. En situaciones de flagrancia o riesgo para la vida o integridad física de NNA, permite además solicitar directamente registros de conexión o datos de registro

95 Disponible en: https://www.impo.com.uy/bases/leyes-originales/20327-2024

96 Disponible en: https://www.unicef.org/brazil/media/37356/file/DH%20Brazil%20Report%20(pt)%20FINAL

97 Disponible en: https://www.lexivox.org/norms/BO-L-N1636.xhtml

98 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

a los proveedores, con control judicial posterior. Cabe resaltar que este tipo de medidas conlleva graves riesgos al ejercicio de derechos humanos en los entornos digitales[99]. La intrusión que pueden implicar estas actuaciones exige delimitar su alcance, duración y condiciones de uso, proteger la información de terceros y establecer garantías frente a la provocación de delitos y la exposición o revictimización de NNA.

Otra dimensión de esta expansión es la conservación de datos sobre personas inocentes. En Paraguay, la Ley 7.549/2025[100] exige conservar durante al menos 12 meses datos de identificación y conexión de las personas usuarias. Aunque excluye el contenido de las comunicaciones y exige una orden judicial para acceder a los registros, la obligación de conservación se aplica de manera general. El control judicial del acceso no elimina los riesgos, por ejemplo, de uso indebido o filtración. Si bien el caso paraguayo refleja una tendencia más amplia en la región[101], la medida ha motivado críticas de organizaciones de la sociedad civil, especialmente cuando las obligaciones de protección trasladan funciones de vigilancia a las propias plataformas. *TEDIC* advirtió que las disposiciones de monitoreo y detección previstas en el proyecto de ley paraguayo sobre *grooming* podrían afectar la privacidad y el cifrado de las comunicaciones y vulnerar derechos fundamentales en el entorno digital[102].

El tratamiento de las herramientas de anonimización constituye otro punto de atención. En Brasil, la Ley 15.487/2026 aumenta entre un tercio y dos tercios la pena cuando determinados delitos se cometen utilizando técnicas de ocultación o anonimización de identificadores digitales para impedir o dificultar la identificación del autor. La medida ha sido criticada por distintas organizaciones de sociedad civil por introducir en el ordenamiento jurídico nacional un tratamiento diferenciado a tecnologías desarrolladas para proteger la privacidad y la seguridad de las personas, como las VPN, pese a una excepción a usos legítimos[103]. Cabe enfatizar que la dificultad para identificar a la per-

99 Ver Derechos Digitales, *Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de vigilancia masiva desplegada por los Estado: casos relevantes en América Latina.* (2024) Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

100 Disponible en: https://silpy.congreso.gov.py/web/ley/146014

101 Ver Díaz, M., *Retención de datos y registro de teléfonos móviles: Chile en el contexto Latinoamericano.* (Derechos Digitales, 2017) Disponible en: https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf

102 "Ley de protección contra el *Grooming*: Cuidar a los niños, niñas y adolescentes, sin vulnerar los derechos digitales", *TEDIC. 29 de octubre de 2025. Disponible en:* https://www.tedic.org/ley-de-proteccion-contra-el-grooming-cuidar-a-los-ninos-ninas-y-adolescentes-sin-vulnerar-los-derechos-digitales/

103 Disponible en: https://www.isoc.org.br/uploads/download/260

sona perpetradora no equivale, por sí misma, a una mayor lesión o riesgo para la víctima. Utilizar herramientas de seguridad como fundamento de agravantes puede estigmatizar su uso y desalentar prácticas de protección necesarias para NNA, periodistas, personas defensoras de derechos humanos y víctimas de violencia. Además, abre espacio para la adopción de medidas similares en otros contextos.

La gravedad de los delitos investigados no exime a los Estados de justificar la necesidad y proporcionalidad de las medidas adoptadas. Esto requiere demostrar su contribución al objetivo perseguido, examinar alternativas menos intrusivas y evaluar sus efectos sobre los derechos de las personas afectadas, incluidos los propios NNA. La protección a este grupo no puede funcionar como una justificación automática para ampliar el acceso a datos personales, normalizar el monitoreo generalizado o debilitar el cifrado y el anonimato. Toda injerencia debe estar prevista en una norma clara, limitarse a lo estrictamente necesario y contar con supervisión independiente y vías efectivas para impugnar abusos. La privacidad y la seguridad digital son condiciones de protección, también para quienes necesitan buscar ayuda, denunciar violencia o comunicarse de manera confidencial.

La expansión de la respuesta penal debe ser considerada, además, en el contexto de los problemas estructurales que caracterizan a los sistemas de justicia penal y penitenciarios de la región. La Comisión Interamericana de Derechos Humanos (CIDH) ha señalado de manera reiterada problemas como el uso excesivo de la prisión preventiva, el hacinamiento y la sobrepoblación, las deficientes condiciones de detención, los altos niveles de violencia y la insuficiencia de servicios básicos, además de las limitaciones para garantizar condiciones adecuadas de reinserción social[104].

Estas condiciones no constituyen un argumento para dejar de investigar y sancionar formas graves de violencia contra NNA. Sí plantean la necesidad de considerar críticamente respuestas que depositan una parte creciente de la política de protección en la expansión de tipos penales y penas privativas de libertad, sin necesariamente fortalecer en la misma medida las capacidades institucionales para prevenir estas violencias, investigarlas adecuadamente y proteger a quienes las sufren.

Así, la respuesta penal y las facultades de investigación deben integrarse en una política de protección que incluya canales accesibles de denuncia, atención psicológica y social, asistencia a víctimas y sus familias, prevención, educación y garantías frente a la revictimización. La eficacia de esa política no puede medirse únicamente por la severi-

104 Comisión Interamericana de Derechos Humanos. *Informe Anual 2025*. (Washington, 2025). Disponible en: https://www.oas.org/es/cidh/docs/anual/2025/IA2025_SPA.pdf; Comisión Interamericana de Derechos Humanos. *Argentina: Uso de la prisión preventiva en la provincia de Córdoba.* (25 de julio de 2025). Disponible en: https://www.oas.org/es/cidh/sesiones/audiencia.asp?Hearing=3845.

dad de las penas o la cantidad de información disponible para las autoridades, sino por su capacidad para reducir las violencias, atender a quienes las sufren y garantizar sus derechos sin producir nuevas vulneraciones.

3.2. Restricciones etarias y la expansión de la determinación de edad

Una segunda tendencia particularmente visible es la proliferación de propuestas que buscan establecer edades mínimas para acceder a redes sociales. Aunque ninguna de las iniciativas de prohibición de acceso identificadas en la región había sido aprobada como ley al cierre del período analizado, este modelo ha ganado rápidamente espacio en las agendas legislativas latinoamericanas.

Con distintas formulaciones, propuestas de este tipo fueron identificadas en Argentina, Brasil, Chile, Colombia, Ecuador, Panamá, Paraguay y Uruguay. Los umbrales no son uniformes: las iniciativas analizadas establecen límites que oscilan entre los 13 y los 16 años y, en algunos casos, combinan edades mínimas con autorización parental para determinados grupos etarios. En Brasil, si bien no han avanzado propuestas de prohibición de acceso a redes sociales, el ECA Digital exige que las cuentas de NNA de hasta 16 años estén vinculadas a las de una persona responsable legal.

En cuanto a las propuestas de prohibición, la velocidad con que circulan entre países contrasta con la evidencia todavía limitada sobre sus implicaciones, particularmente en los contextos latinoamericanos. Evaluar estas medidas requiere considerar tanto su capacidad para reducir la exposición a determinados riesgos como las formas concretas en que NNA acceden a internet en la región. Condiciones socioeconómicas, desigualdades territoriales, disponibilidad de dispositivos y posibilidades de acompañamiento familiar afectan las formas de acceso y uso de tecnologías. La evidencia regional refuerza, además, que los usos problemáticos resultan de múltiples factores, entre ellos el tiempo y la intensidad de uso, el acceso temprano, el bienestar, las dinámicas familiares y los contextos de socialización[105]. Por ello, modelos desarrollados en otros contextos no deberían ser simplemente reproducidos sin evidencia sobre sus posibles efectos diferenciados en América Latina.

Las restricciones etarias introducen, además, una segunda cuestión regulatoria: para impedir que una persona con determinada edad utilice un servicio es necesario establecer algún mecanismo para determinar su edad. Por eso, las propuestas de prohibición o restricción aparecen en general acompañadas de obligaciones de verificación o estima-

105 Matías Dodel, Ariel Tófalo, Rolando Pérez, David Torres y Jazmín Mazó Torrico. *Usos problemáticos de dispositivos digitales en la infancia y adolescencia en América Latina: desigualdad, bienestar y apoyo familia.* CEPAL. (Santiago, 2026). Disponible en: https://www.cepal.org/es/publicaciones/90361-usos-problematicos-dispositivos-digitales-la-infancia-adolescencia-america

ción etaria. Sin embargo, la relación entre condicionamientos por edad y obligaciones de determinación no es uniforme.

La determinación de edad comprende distintos procedimientos para verificar o estimar la edad o el rango etario de una persona. La verificación utiliza documentos oficiales u otras fuentes acreditadas para comprobar la edad, sin que necesariamente deba revelarse la identidad completa al servicio. La estimación, en cambio, infiere una edad probable mediante el análisis de características físicas, como la apariencia facial, o de señales de comportamiento, como las interacciones con dispositivos, los patrones de uso y la actividad en una plataforma[106]. Esta distinción es relevante porque los métodos requieren distintos datos y presentan diferentes márgenes de error y riesgos para los derechos.

Los mecanismos disponibles para determinar la edad de las personas usuarias incluyen desde la presentación o comprobación de documentos de identidad hasta sistemas de estimación etaria basados en biometría o en patrones de uso. Las iniciativas analizadas no siempre determinan qué tecnología deberá utilizarse para cumplir con las obligaciones de determinación. Algunas, sin embargo, incorporan salvaguardas específicas para reducir la cantidad de datos personales compartidos. El proyecto de ley argentino 2.733-D-2026[107], por ejemplo, prevé una tecnología estatal que informaría a las plataformas únicamente si una persona supera o no el umbral de edad aplicable, sin transferir datos como el número de documento, el domicilio, una imagen biométrica o la fecha exacta de nacimiento.

Más allá del método utilizado, la determinación de edad constituye un ejemplo claro de cómo una regulación dirigida a la protección de NNA puede alterar la infraestructura y las condiciones de acceso a internet para todas las personas. Eso porque, para distinguir quién cumple un umbral etario, es necesario recolectar información también de personas adultas que no son objeto de la legislación. Con eso, el acceso a servicios digitales —que actualmente no son necesariamente mediados por una acreditación de edad o de identidad— queda sujeto a exigencias que tienen implicaciones críticas para la participación digital, la privacidad, la libertad de expresión y el acceso a información. Cabe resaltar que la vulneración de estos derechos afecta también a las infancias que se busca proteger. De este modo, la medida puede debilitar el mismo propósito de la política de protección.

106 OCDE. "AGE ASSURANCE PRACTICES OF 50 ONLINE SERVICES USED BY CHILDREN". (París: june 2025). Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/age-assurance-practices-of-50-online-services-used-by-children_3fbe5e92/a19853ab-en.pdf

107 Disponible en: https://www.hcdn.gob.ar/comisiones/permanentes/ceducacion/proyecto.html?exp=2733-D-2026

El problema no consiste en la pérdida de un anonimato absoluto que hoy estuviera garantizado. La mayoría de las conexiones y dispositivos ya generan identificadores y registros que pueden permitir rastrear actividades y, bajo determinadas condiciones, asociarlas con una persona. Sin embargo, dejar rastros no equivale a tener que identificarse, ni a que toda actividad esté directamente vinculada a una identidad acreditada. El acceso a información identificatoria debe estar sujeto a garantías y, como regla general, a autorización judicial. Además, la identificación debe darse en casos específicos y en la forma determinada por ley, cuando sea estrictamente necesario para los fines buscados y de manera proporcional. La comprobación de edad generalizada invierte la lógica de la identificación como una medida excepcional. No es aceptable una generalización de comprobaciones de edad como condición cotidiana de acceso a internet.

No todos los sistemas de determinación etaria producen esa asociación de la misma manera. Una credencial que acredita únicamente el cumplimiento de un umbral puede reducir la información que recibe la plataforma. Pero limitar los datos compartidos no resuelve por sí solo quién conoce la identidad al emitir la credencial, si las comprobaciones pueden vincularse entre servicios o si quedan registros que permitan reconstruir dónde y cuándo fue utilizada. Por ello, las salvaguardas deben examinar el funcionamiento del sistema completo y garantizar que la comprobación de edad no se convierta en una infraestructura de seguimiento de la navegación.

A esta transformación se suman los riesgos específicos de cada método[108]. Los procedimientos basados en documentos pueden excluir a quienes no cuentan con la documentación admitida o no pueden completar la comprobación, por ejemplo. Los que analizan imágenes faciales requieren procesar datos sensibles, mientras que la estimación basada en comportamientos puede incentivar un análisis más intensivo de la actividad digital. Estos últimos métodos también plantean dificultades cuando varias personas utilizan un mismo dispositivo, una práctica relevante en contextos de desigualdad de acceso como los latinoamericanos. Si la estimación se basa en la actividad del dispositivo o de una cuenta compartida, puede combinar patrones de uso de distintos integrantes de una familia y atribuir a una persona la edad inferida a partir del comportamiento de otra. Esto puede tanto restringir injustificadamente el acceso de personas adultas como impedir que se activen las protecciones correspondientes a NNA. Además, los resultados de la estimación son probabilísticos. Evaluaciones técnicas de sistemas de estimación facial han encontrado diferencias de desempeño según la edad, el sexo, la región de origen y la calidad de la imagen. Estos errores pueden traducirse en exclusiones injustificadas o en la exigencia de comprobaciones adicionales más intrusivas.

108 Marina Meira. “Por que aplicar a verificação de idade na internet é tão difícil”, *UOL Tilt*. 7 de octubre de 2025. Disponible en: https://www.uol.com.br/tilt/analises/ultimas-noticias/2025/10/07/por-que-aplicar-a-verificacao-de-idade-na-internet-e-tao-dificil.htm

La incorporación de proveedores especializados para realizar esos servicios introduce, además, nuevos actores y flujos de datos. Sin salvaguardas, la información obtenida puede conservarse, combinarse con otros registros o reutilizarse para perfilamiento, publicidad y otras finalidades comerciales o de vigilancia. Esta explotación constituye un riesgo adicional, pero el problema central persiste incluso cuando los datos no se comercializan. Las garantías de minimización, separación de finalidades y eliminación de datos son indispensables, pero deben acompañarse de una evaluación previa de si la exigencia resulta necesaria y proporcional para cada servicio.

La consideración de estos riesgos no es uniforme en las iniciativas legales analizadas. Algunas incorporan salvaguardas específicas, como el proyecto argentino 2733-D-2026[109], que limita la información comunicada a las plataformas al cumplimiento del umbral etario, o el proyecto peruano 00498/2026-2031-CD[110], que exige una alternativa a los documentos oficiales y restringe el uso y la conservación de los datos obtenidos. Otras establecen obligaciones de determinación de edad sin precisar suficientemente los límites del tratamiento de datos ni las garantías exigibles a los proveedores que intervienen[111]. También varía el alcance de la exigencia. En Brasil, la ley y su decreto reglamentario[112] contemplan obligaciones diferenciadas según las características de los servicios y contenidos, en lugar de exigir indiscriminadamente la determinación de edad para acceder a cualquier espacio digital. Estas diferencias son relevantes, aunque tanto la delimitación de los servicios sujetos a comprobación como las salvaguardas de datos deben evaluarse a la luz de la necesidad y proporcionalidad de la medida y de sus efectos sobre los derechos.

Estos problemas no son exclusivos de América Latina, aunque las condiciones regionales pueden intensificarlos. Las desigualdades en el acceso a documentos, dispositivos y servicios digitales pueden dificultar las comprobaciones y agravar sus efectos excluyentes. Asimismo, la articulación de estos mecanismos con infraestructuras estatales y privadas de identificación requiere especial atención a los controles sobre el acceso, la vinculación y la reutilización de datos. La evaluación regional debe considerar tanto estas condiciones como el cambio más amplio que supone convertir la determinación

109 Disponible en: https://www.hcdn.gob.ar/comisiones/permanentes/ceducacion/proyecto.html?exp=2733-D-2026

110 Disponible en: https://img.lpderecho.pe/wp-content/uploads/2026/10/PL-00498-2026-2031-CD-LP-Derecho.pdf

111 Por ejemplo, el Proyecto de Ley 2387/2025, de Brasil, y la versión original del Proyecto de Ley 10880/2024-CR, de Perú.

112 Disponibles en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm; https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

de edad en un requisito habitual para informarse, comunicarse y participar en internet.

3.3. De restringir el acceso a regular los servicios digitales

Paralelamente, el mapeo muestra otra tendencia regulatoria: la adopción o discusión de marcos más amplios que trasladan parte de la responsabilidad hacia las empresas que diseñan y operan productos y servicios digitales. Ejemplos en la región incluyen el caso brasileño y colombiano —en distinta medida—, los proyectos discutidos en Argentina, Chile, México, Panamá y Perú.

Estas iniciativas amplían el objeto de la regulación. Además de las condiciones de acceso de NNA a determinados servicios, incorporan cuestiones como privacidad y seguridad por diseño, configuraciones protectoras por defecto, sistemas de recomendación, patrones oscuros, diseño orientado a maximizar el tiempo de permanencia, publicidad comportamental, perfilamiento y tratamiento de datos personales. Este enfoque reconoce que determinados riesgos no dependen únicamente de las conductas de las personas usuarias, sino también de las características de los productos y de los modelos de negocio que los sostienen. Permite, por tanto, orientar la intervención hacia las decisiones corporativas que generan o intensifican esos riesgos y ampliar el debate más allá de la oposición entre permitir o prohibir el acceso a redes sociales. Ambos enfoques pueden coexistir, como muestra el ECA Digital brasileño, que combina obligaciones sobre el funcionamiento de los servicios con limitaciones a la creación de cuentas individuales por NNA de hasta 16 años.

Al mismo tiempo, las experiencias analizadas muestran tensiones que generaron cuestionamientos de organizaciones de la sociedad civil frente a obligaciones excesivamente amplias de monitoreo, moderación, identificación de personas usuarias o retiro de contenidos, que pueden afectar la privacidad, la libertad de expresión, el acceso a información y la seguridad de las comunicaciones[113].

El desafío de estos modelos es, por lo tanto, avanzar en la responsabilidad de las empresas por las condiciones de los entornos digitales que diseñan y operan, sin transformar la protección de NNA en una autorización general para ampliar mecanismos de vigilancia,

113 "*ISOC Chile* presenta Evaluación de Impacto en Internet sobre proyecto de ley de protección de NNA en entornos digitales", *ISOC CHILE*. 31 de agosto de 2026. Disponible en: https://www.isoc.cl/?p=5946; "Proteger a niños, niñas y adolescentes sin sacrificar derechos: lo que preocupa del decreto que reglamenta la Ley 2489 de 2025", Fundación Karisma. 19 de mayo de 2026. Disponible en: https://blog.karisma.org.co/proteger-a-ninos-ninas-y-adolescentes-sin-sacrificar-derechos-lo-que-preocupa-del-decreto-que-reglamenta-la-ley-2489-de-2025/; Rubiela Gaspar. "Hacia una Internet Segura: regular sin censurar a infancias y adolescencias", Hiperderecho. Disponible en: https://hiperderecho.org/2025/06/hacia-una-internet-segura-regular-sin-censurar-a-infancias-y-adolescencias/

control de contenidos o recopilación de datos. La regulación del diseño y de los modelos de negocio abre una agenda importante para la región, pero exige que las obligaciones sean específicas, proporcionales a los riesgos y acompañadas de salvaguardas claras para los derechos de NNA y de las demás personas usuarias.

Su implementación requiere, además, construir y fortalecer una institucionalidad capaz de supervisar el cumplimiento de esas obligaciones. No basta con atribuir nuevas competencias a las autoridades si estas carecen de independencia frente a intereses políticos y empresariales, conocimientos técnicos y recursos financieros y humanos suficientes. La supervisión debe contar con facultades para obtener información de las empresas, evaluar sus prácticas y exigir medidas correctivas, junto con mecanismos de coordinación entre las autoridades de protección de datos, consumo y derechos de NNA. La transparencia, la rendición de cuentas y la participación de la sociedad civil y de los propios NNA deben acompañar esta construcción institucional, para que la protección no dependa exclusivamente de las evaluaciones y decisiones de las empresas reguladas.

3.4. Dos agendas emergentes: participación en actividades económicas digitales e inteligencia artificial

Además de las tendencias anteriores, el mapeo identifica dos agendas que comienzan a adquirir un tratamiento más específico en la región. La primera se refiere a la participación de NNA en actividades económicas digitales. La segunda, a las implicaciones de la inteligencia artificial para sus derechos. Aunque ambas se conectan con problemas previos, plantean nuevas preguntas sobre las responsabilidades de empresas, familias y autoridades.

La participación de NNA como creadores de contenido digital plantea cuestiones específicas sobre la explotación comercial de su imagen y voz, las condiciones de producción, la administración de ingresos y las responsabilidades de familias, plataformas y anunciantes. Durante el período analizado, este tema recibió atención regulatoria en Brasil, cuyo decreto reglamentario del ECA Digital[114] exige autorización judicial previa para determinadas formas de explotación habitual de la imagen o rutina de NNA en contenidos monetizados o promocionados; Ecuador, donde un proyecto presentado en 2026 propone salvaguardas patrimoniales y mecanismos de debida diligencia frente a la explotación económica y sobreexposición de NNA[115]; y Colombia, donde el Proyecto

114 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm

115 Disponible en: https://www.asambleanacional.gob.ec/es/noticia/118087-luigi-garcia-impulsa-ley-para-proteger-ninas-ninos-y

de Ley 394/2025C[116] combina la protección de NNA en entornos digitales con la regulación de creadores de contenido.

Aunque incipiente en la región, esta agenda cuenta con antecedentes internacionales. Francia, por ejemplo, adoptó en 2020 una legislación específica sobre la explotación comercial de la imagen de personas con menos de 16 años en plataformas en línea[117], extendiendo protecciones tradicionalmente asociadas al trabajo infantil en sectores audiovisuales a determinadas actividades realizadas en plataformas digitales y estableciendo reglas específicas para la generación de ingresos y difusión de contenidos.

La aparición de estas iniciativas sugiere una ampliación adicional de la agenda de protección digital. NNA participan de las plataformas como personas usuarias expuestas a contenidos e interacciones, pero también como productores de contenido y actores de una economía digital capaz de generar valor a partir de su imagen, actividad y datos. El desafío consiste en garantizar que esta participación respete sus derechos, incluyendo las condiciones de producción, la protección de sus ingresos, su privacidad y sus posibilidades de decidir sobre la exposición de su imagen.

La segunda agenda emergente se refiere a la inteligencia artificial. Hasta el momento, buena parte de las respuestas identificadas se concentra en su utilización para facilitar formas de violencia sexual. Brasil, mediante la Ley 15.487/2026[118], y Perú, mediante la Ley 32.314/2025[119], incorporaron expresamente contenidos producidos o manipulados con IA en sus disposiciones sobre material de abuso sexual infantil. En México[120] y Ecuador[121] también se identificaron proyectos dirigidos a sancionar representaciones sexuales generadas mediante estas tecnologías o su utilización para facilitar el engaño y el contacto con NNA con fines sexuales. Estas iniciativas muestran una adaptación

116 Disponible en: https://leyes.senado.gov.co/p-ley/2024-2025/PL%20394-25%20CONTENIDO%20DIGITAL.pdf

117 Disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054

118 Disponible en: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm

119 Disponible en: https://img.lpderecho.pe/wp-content/uploads/2025/04/Ley-32314-LPDerecho.pdf

120 Iniciativa que reforma y adiciona diversas disposiciones del Código Penal Federal, de la Ley General de Educación y de la Ley General de los Derechos de Niñas, Niños y Adolescentes, en materia de protección digital e inducción sexual mediante engaño. Disponible en: https://gaceta.diputados.gob.mx/PDF/66/2026/mar/20260318-II-3.pdf

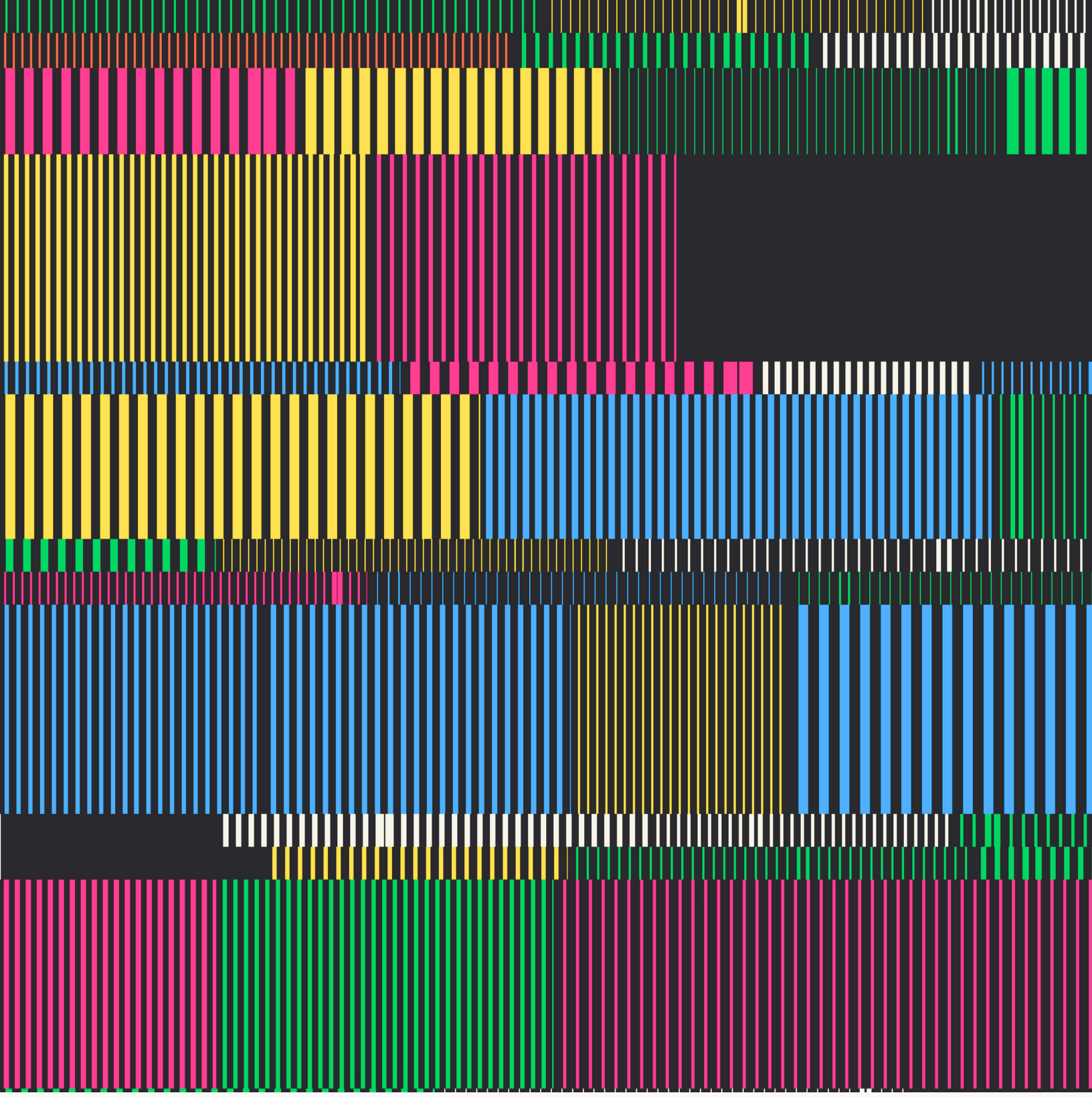
121 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/115385-proyecto-de-ley-organica-reformatoria

de los marcos penales a nuevas formas de producción y circulación de contenidos y de interacción con las víctimas.

Sin embargo, la agenda de IA y derechos de NNA no se agota en la respuesta penal. En Ecuador, el Proyecto de Ley Orgánica de Aprovechamiento Digital e Inteligencia Artificial para Niñas, Niños y Adolescentes[122] proponía un marco específico que incluye transparencia, responsabilidad, protección de datos, seguridad y acceso equitativo. Su inclusión en el mapeo permite identificar una línea de discusión que abarca también las condiciones de diseño, desarrollo y utilización de sistemas de IA que pueden afectar a NNA.

Esta ampliación resulta relevante porque los impactos de la IA sobre NNA exceden la generación de contenidos sexuales. También requieren examinar cómo estos sistemas intervienen en el aprendizaje, el acceso a información, las interacciones y las decisiones que les afectan, así como los riesgos de discriminación, perfilamiento y explotación comercial de sus datos. Una agenda de protección integral debe abordar estas dimensiones y establecer responsabilidades a lo largo del desarrollo y uso de los sistemas, con garantías de transparencia, supervisión y participación de NNA. De lo contrario, la atención a las manifestaciones más visibles de violencia puede dejar fuera del debate otros efectos sobre sus derechos.

122 Disponible en: https://www.asambleanacional.gob.ec/es/multimedios-legislativos/101492-proyecto-de-ley-organica-de



04

CONSIDERACIONES FINALES

04

4. CONSIDERACIONES FINALES

El panorama analizado en este informe muestra la creciente centralidad de la protección de niñas, niños y adolescentes en entornos digitales en las agendas regulatorias de América Latina. En un período relativamente corto, distintos países aprobaron nuevas leyes, reformaron marcos existentes o comenzaron a discutir iniciativas dirigidas específicamente a la relación entre NNA y tecnologías digitales. Aunque estas respuestas parten de preocupaciones legítimas frente a riesgos y formas de violencia que requieren atención pública, el mapeo muestra también una considerable diversidad en los problemas identificados y en las soluciones propuestas.

Al mismo tiempo, esta agenda tiene implicaciones que exceden la protección de NNA. Algunas de las medidas analizadas intervienen directamente sobre la forma en que servicios digitales son diseñados y operados, las condiciones para acceder a ellos, los datos que deben recopilarse de las personas usuarias y las reglas aplicables a la circulación y moderación de contenidos. En este sentido, las decisiones regulatorias adoptadas en nombre de la protección de NNA se inscriben, como ha ocurrido históricamente, en debates más amplios sobre la gobernanza de internet[123] y pueden producir efectos sobre el ejercicio de derechos humanos por parte del conjunto de la población.

La protección de NNA no ocurre al margen de los demás derechos reconocidos por la Convención sobre los Derechos del Niño. NNA tienen, entre otros, derecho a la privacidad, a buscar y recibir información, a expresarse, participar y asociarse y a ejercer niveles crecientes de autonomía de acuerdo con el desarrollo de sus capacidades. El Comité de los Derechos del Niño ha subrayado precisamente que estos derechos continúan siendo aplicables en los entornos digitales. Las medidas regulatorias deben, por lo tanto, proteger frente a daños y preservar las condiciones para el ejercicio de esos derechos.

Pero el análisis de derechos humanos tampoco termina en los derechos de NNA. Varias de las medidas identificadas en este informe requieren modificaciones técnicas o regulatorias que alcanzan al conjunto de las personas usuarias de internet. La determinación de edad ofrece un ejemplo particularmente claro: una obligación creada para distinguir qué personas pueden acceder a determinado servicio puede llevar a introducir mecanismos de comprobación o estimación de edad en una escala mucho mayor y modificar las condiciones de acceso también para personas adultas. De forma similar, obliga-

123 Jovan Kurbalija. *An Introduction to Internet Governance*. (DiploFoundation, 2016). Disponible en: https://dspace.diplomacy.edu/items/be5449e5-a1c3-4e42-bf53-2ce6c1b0cc49

ciones relacionadas con la detección y moderación de contenidos pueden afectar la libertad de expresión y el acceso a la información de otras personas usuarias, mientras que medidas que impliquen monitoreo de comunicaciones o debilitamiento de mecanismos de seguridad pueden generar consecuencias para la privacidad y seguridad de las comunicaciones de toda la población.

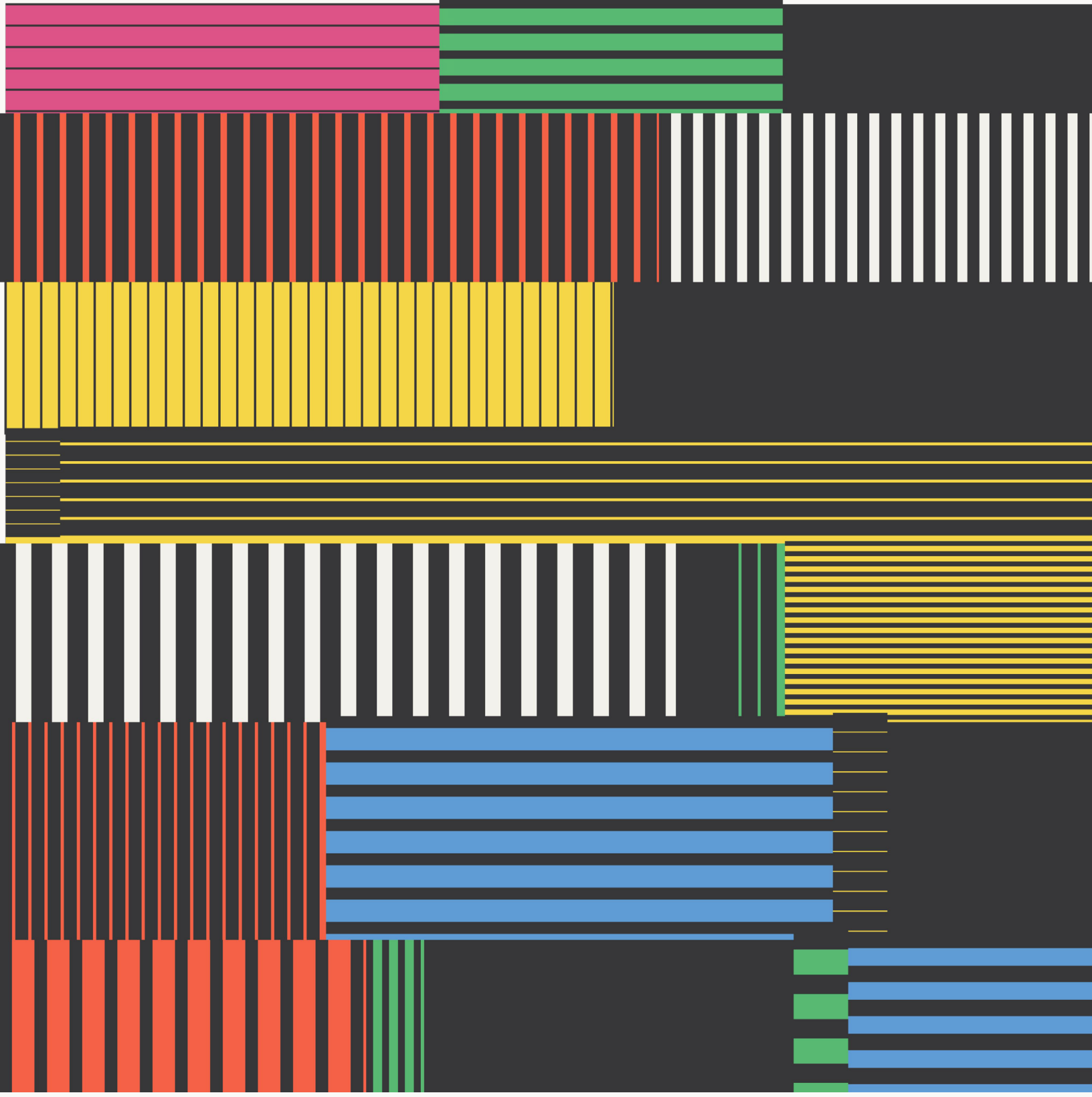
Esto muestra la importancia de evaluar estas medidas no solamente a partir de la legitimidad del objetivo de protección que persiguen, sino también de su proporcionalidad, de sus efectos previsibles sobre diferentes derechos y de la existencia de alternativas menos restrictivas. El alcance de una obligación, los mecanismos utilizados para implementarla, las categorías de servicios a las que se aplica y las salvaguardas incorporadas pueden determinar impactos muy diferentes sobre derechos humanos. Esta evaluación debe acompañarse de capacidades institucionales para supervisar su implementación y de mecanismos de participación que incorporen las experiencias y perspectivas de NNA.

La protección de NNA y los derechos digitales no deben plantearse como objetivos contrapuestos. Los derechos humanos ofrecen tanto el fundamento de la protección como los parámetros para determinar cómo hacerla efectiva y cuáles son los límites de las medidas adoptadas. Esto exige considerar los derechos de NNA desde una perspectiva integral y evaluar los efectos de las transformaciones en la infraestructura, el diseño y la gobernanza de los servicios sobre internet como espacio para el ejercicio de derechos.

Una agenda latinoamericana debe, además, aprovechar los aprendizajes internacionales sin reproducir automáticamente sus soluciones. Los enfoques europeos sobre responsabilidades empresariales y el modelo australiano de restricción etaria ya influyen en la región, pero su adopción no traslada las condiciones institucionales, sociales y económicas necesarias para implementarlos. La producción de evidencia regional resulta indispensable para evaluar sus efectos en contextos de desigualdad de acceso y capacidades regulatorias diversas. También deben considerarse las asimetrías de poder entre países y frente a las empresas transnacionales, que utilizan su capacidad económica y sus estructuras de lobby para influir en las decisiones públicas y limitar las obligaciones que se les imponen. Esto exige transparencia sobre esa influencia y garantías frente a la captura de los procesos regulatorios.

Fortalecer la cooperación regional puede contribuir a reducir esas asimetrías mediante el intercambio de evidencia, la coordinación entre autoridades y la construcción conjunta de capacidades para supervisar servicios que operan más allá de las fronteras nacionales. Esa articulación debe apoyarse en instituciones independientes, recursos suficientes y participación efectiva de la sociedad civil y de los propios NNA. Una agenda verdaderamente latinoamericana requiere que las expe-

riencias, necesidades y desigualdades de la región orienten las respuestas, y que la responsabilidad de proteger se distribuya sin descargarla en las familias ni dejarla a la voluntad de las empresas. Su resultado debe evaluarse por la reducción de las violencias y la ampliación de las condiciones para ejercer derechos.



Derechos Digitales
AMÉRICA LATINA