Paola Isabel Martínez Paitán
Diputada de la República

CÁMARA DE DIPUTADOS
CONGRESO DEL PERÚ

CÁMARA DE DIPUTADOS
ÁREA DE TRÁMITE DOCUMENTARIO
RECIBIDO
PROPOSICIÓN LEGISLATIVA
00780-2026-2031-CD
RU 60203-CD
06 NOVIEMBRE 2026 09:45 a. m.
FIRMADO DIGITALMENTE: EBOHORQUEZ

PROPOSICIÓN LEGISLATIVA SOBRE LA PROTECCIÓN DE LA SALUD MENTAL Y BIENESTAR DIGITAL DE NIÑOS Y ADOLESCENTES EN ENTORNOS DIGITALES

La Diputada de la República que suscribe, **PAOLA ISABEL MARTÍNEZ PAITÁN,** integrante del Grupo Parlamentario **RENOVACIÓN POPULAR**, en el ejercicio del derecho de iniciativa legislativa que le confiere el artículo 107° de la Constitución Política del Perú y conforme lo establecen los artículos 98º y 107º del Reglamento de la Cámara de Diputados del Congreso de la República, presenta la siguiente **PROPOSICIÓN LEGISLATIVA**:

LEY DE PROTECCIÓN DE LA SALUD MENTAL Y BIENESTAR DIGITAL DE NIÑOS Y ADOLESCENTES EN ENTORNOS DIGITALES

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley

La presente ley tiene por objeto establecer un marco regulatorio para el uso seguro, responsable y saludable de los entornos digitales y servicios en línea por niños y adolescentes, a fin de reducir riesgos y proteger su desarrollo integral; así como regular las medidas de prevención y orientación para los padres y tutores, y las obligaciones aplicables a las entidades públicas, a las empresas operadoras de servicios públicos de telecomunicaciones y a los proveedores de servicios digitales.

Artículo 2. Finalidad de la Ley

La presente ley tiene por finalidad lo siguiente:

a) Proteger la salud mental y el desarrollo cognitivo, emocional y social de niños y adolescentes ante el uso excesivo o adictivo de dispositivos y servicios digitales, incluyendo prácticas de diseño potencialmente adictivas asociadas a ansiedad, depresión, alteraciones del sueño, problemas de autoestima y socialización, entre otros.

b) Prevenir la exposición a contenidos nocivos, tales como violencia, discursos de odio, autolesiones, suicidio, pornografía e información falsa, entre otros.

c) Reducir el riesgo de victimización de niños y adolescentes en delitos y conductas de alto riesgo en línea, tales como el ciberacoso, el grooming, la sextorsión, la difusión no consentida de imágenes íntimas, la suplantación de identidad y el uso malicioso de contenidos sintéticos generados mediante inteligencia artificial, así como frente a interacciones en línea no solicitadas y persistentes de riesgo, entre otros.

d) Garantizar la privacidad digital y la protección de datos personales de niños y adolescentes, conforme a la Ley 29733, Ley de Protección de Datos Personales, y su reglamento.

e) Fortalecer la ciudadanía digital y el bienestar de niños y adolescentes, así como de sus padres, madres o tutores.

Artículo 3. Ámbito de aplicación

3.1. La presente ley se aplica a los siguientes sujetos:

a) Las entidades públicas de los tres niveles de gobierno cuyas competencias se vinculen al uso seguro, responsable y saludable de las tecnologías digitales y de los entornos digitales por niños y adolescentes.

b) Las empresas operadoras de servicios públicos de telecomunicaciones que prestan servicios de acceso a internet en el territorio nacional y aquellas que provean wi fi gratuito en locales comerciales y espacios públicos.

c) Los proveedores de servicios digitales que ofrezcan o pongan a disposición sus servicios en el mercado peruano, incluidos aquellos que, sin contar con presencia física en el país, los dirijan a usuarios ubicados en el territorio nacional, a través de plataformas digitales y redes sociales, tiendas de aplicaciones, sistemas operativos o videojuegos, conforme a la normativa vigente.

3.2. Las personas naturales y jurídicas de derecho privado se sujetan a lo dispuesto en esta ley, en lo que les sea aplicable, así como a las obligaciones derivadas de su vinculación con el Estado.

3.3. Los proveedores de servicios digitales sin domicilio en el país, quienes designan un representante legal en el territorio nacional para la recepción de notificaciones y la atención de los requerimientos de las autoridades competentes, conforme al reglamento.

Artículo 4. Definiciones

Para efectos de la presente ley, se adoptan las siguientes definiciones:

a) Módulo "Modo Aprendizaje". Conjunto de herramientas, recursos y guías digitales de referencia promovidas por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, orientadas a fomentar el uso seguro, saludable y educativo de los entornos digitales por niños y adolescentes. La iniciativa agrupa y difunde soluciones que permiten establecer perfiles por grupos etarios, limitación de tiempo de uso, suspensión o restricción de notificaciones y de funcionalidades potencialmente adictivas, tales como reproducción automática, desplazamiento infinito y rachas, así como la posibilidad de restringir el descubrimiento y la mensajería directa. Su diseño y promoción se rigen por los principios de minimización de datos, privacidad y seguridad por defecto y no inspección del contenido de comunicaciones. Los parámetros técnicos mínimos y criterios de certificación voluntaria de herramientas incluidas en la iniciativa se establecen en el reglamento de la presente ley.

b) Bienestar digital. Estado de equilibrio en el uso de tecnologías y servicios digitales que permite al niño y adolescente desarrollar sus actividades cotidianas, sociales, educativas y recreativas de manera saludable, segura y responsable, sin afectar su salud física, mental ni sus relaciones interpersonales, en concordancia con las políticas nacionales de salud mental y ciudadanía digital.

c) Ciberacoso o *cyberbullying*. Es el delito que perpetrado por quien, de forma reiterada o valiéndose de tecnologías de la información, vigila, persigue u hostiga a una persona alterando su vida cotidiana. Se encuentra tipificado en el artículo 151-A del Código Penal o norma que la sustituya.

d) *Deepfake* o ultrafalso. Contenido multimedia (vídeo, audio o imagen) manipulado o generado mediante inteligencia artificial y técnicas de aprendizaje profundo (*deep learning*) que hace parecer real algo que nunca ocurrió.

e) Dispositivo móvil. Equipo electrónico portátil, personal y de uso inalámbrico que permite acceder a servicios digitales o de telecomunicaciones, incluyendo teléfonos celulares, tabletas, computadoras portátiles y dispositivos inteligentes análogos, conforme a la clasificación técnica establecida por el Ministerio de Transportes y Comunicaciones y la Secretaría de Gobierno y Transformación Digital.

f) Funcionalidades de uso continuado. Características del diseño de un servicio digital que fomentan su uso prolongado o repetitivo, tales como la reproducción automática, el desplazamiento infinito, las rachas, las recompensas variables y las notificaciones persuasivas**.**

g) "Grooming" o captación sexual de menores en entornos digitales. Proceso deliberado por el cual una persona adulta contacta a un niño o adolescente por medios digitales, gana su confianza mediante engaño, manipulación o seducción, y busca involucrarle en actividades de naturaleza sexual. Puede incluir solicitud de material sexual, conversaciones sexualizadas o intentos de concertar encuentros fuera de línea. Esta modalidad se relaciona con las proposiciones con fines sexuales por medios tecnológicos previstas en el ordenamiento peruano.

h) Marcador de estado "dispositivo utilizado por un niño o adolescente". Atributo binario, activo o inactivo, asociado a un equipo con servicio público de telecomunicaciones o a su perfil SIM o eSIM equivalente, que indica exclusivamente que el dispositivo ha sido declarado para uso habitual por un niño y adolescente. No contiene datos de identidad del menor ni de tráfico, ubicación o contenidos, y se utiliza únicamente para habilitar configuraciones protectoras por defecto y canalizar controles parentales. Su activación, suspensión o revocación se efectúa por el titular del servicio.

i) Proveedor de servicios digitales. Persona natural o jurídica que ofrece o pone a disposición del público en el mercado peruano plataformas y redes sociales, videojuegos en línea, tiendas de aplicaciones, sistemas operativos, sistemas de inteligencia artificial conversacional u otros servicios en línea, con independencia de su lugar de establecimiento.

j) Registro de dispositivos móviles de uso por niños y adolescentes (RDU-NA). Banco de datos de finalidad única que consigna, de manera pseudonimizada, el marcador de estado de dispositivos declarados para uso habitual por personas menores de dieciocho años, la constancia de consentimiento verificable del titular del dispositivo móvil y la línea de servicio, así como los metadatos estrictamente necesarios para gestionar su activación, actualización y revocación.

El RDU-NA no incorpora datos de identidad del niño o adolescente, números de línea, geolocalización, tráfico ni contenidos.

k) Sextorsión o chantaje sexual. Es la modalidad de violencia sexual en la que una persona amenaza o intimida, por cualquier medio, incluidas las tecnologías digitales, con publicar o difundir imágenes, videos o audios íntimos para obtener dinero, favores sexuales u otros beneficios, o forzar conductas de connotación sexual. Esta conducta delictiva se encuentra tipificada en el artículo 176-C del Código Penal o, en su defecto, en la norma que la sustituya.

l) Titular del dispositivo móvil. Es la persona natural mayor de edad o la persona jurídica registrada oficialmente como abonado o usuario de la línea telefónica y propietaria del equipo ante el operador de telecomunicaciones. El titular responde administrativamente por el cumplimiento de las obligaciones contractuales y la veracidad de la declaración de uso de la línea por menores de edad, y civilmente conforme a las reglas del Código Civil por los daños derivados del incumplimiento de sus deberes de custodia

CAPÍTULO II

REGLAS DE ACCESO PARA EL USO DE DISPOSITIVOS MOVILES, SERVICIOS DIGITALES Y CORRESPONSABILIDAD DE LAS FAMILIAS

Artículo 5. Acceso de menores de edad a dispositivos móviles, plataformas y servicios digitales

5.1. El acceso y uso de dispositivos móviles por menores de edad se realiza bajo la orientación y supervisión del padre, madre, tutor o representante legal, considerando su edad, grado de madurez y autonomía progresiva. Para promover un uso seguro y saludable, se establecen las siguientes orientaciones:

a) Menores de doce años: se recomienda que el uso de dispositivos móviles se realice bajo supervisión directa de padres, tutores o una persona adulta y se priorice para fines educativos o situaciones de emergencia. En la primera infancia, especialmente de 0 a 3 años, se recomienda evitar o reducir la exposición a pantallas; entre los tres y seis años se recomienda evitar el acceso a dispositivos móviles; entre los seis y doce años todo uso debe ser supervisado por adultos.

b) De doce a menos de dieciséis años: se recomienda priorizar el uso educativo y limitar el uso recreativo o no educativo a un máximo de dos horas diarias, mediante controles parentales y configuraciones de restricción del tiempo disponibles a nivel de sistema operativo o de la plataforma digital.

c) De dieciséis a menos de dieciocho años: se promueve el uso responsable y progresivamente autónomo de los dispositivos móviles, recomendándose limitar el uso recreativo o no educativo a un máximo de dos horas diarias, sin perjuicio de las actividades educativas, de comunicación y otras necesidades justificadas.

5.2. Para el acceso a plataformas y servicios digitales se establecen las siguientes reglas:

a) Las personas de dieciséis a menos de dieciocho años pueden abrir y gestionar cuentas propias en servicios y plataformas digitales, debiendo disponer de herramientas accesibles para limitar el uso no educativo, establecer períodos de descanso y desactivar notificaciones no esenciales.

b) Las personas menores de dieciséis años acceden y utilizan servicios digitales con autorización y supervisión de su padre, madre, tutor o representante legal, priorizando contenidos educativos, controlando su uso mediante restricciones temporales, bloqueos o filtros a nivel del sistema operativo o de la plataforma digital.

c) Los mecanismos de verificación o aseguramiento de la edad deben ser proporcionales a los riesgos del servicio y observar la Ley 29733, Ley de Protección de Datos Personales, y su reglamento.

d) El tratamiento de datos personales de menores de edad se limita a las finalidades legítimas y a los datos necesarios conforme a la legislación vigente. El tratamiento para finalidades adicionales requiere el consentimiento que corresponda. Se prohíbe la publicidad dirigida a menores de edad basada en la elaboración de perfiles a partir de sus datos personales.

e) La implementación de perfiles para niños y adolescentes de protección, controles parentales y mecanismos de verificación de edad y configuraciones por defecto no autoriza la inspección del contenido de comunicaciones privadas ni el tratamiento de datos personales, reguladas mediante la Ley 29733 y a la normativa de neutralidad de red aplicable.

Artículo 6. Orientaciones para el padre, madre o tutor

El padre, madre o tutor, en ejercicio de sus responsabilidades de cuidado y protección, debe adoptar medidas de acompañamiento, orientación y supervisión del uso de dispositivos móviles, plataformas y servicios digitales por menores de edad, considerando su edad, grado de madurez y autonomía progresiva, conforme a los siguientes lineamientos:

6.1. Promover hábitos saludables de utilización de dispositivos móviles y servicios digitales, estableciendo límites razonables respecto del tiempo de uso, los horarios de conexión y el acceso a contenidos que puedan afectar la salud mental, el descanso, el rendimiento educativo o el desarrollo integral de los menores de edad.

6.2. Fomentar la comunicación familiar y el diálogo permanente sobre los riesgos de los entornos digitales, incluyendo el ciberacoso, la captación con fines sexuales, la sextorsión, la exposición a contenidos perjudiciales y otras situaciones que puedan comprometer la integridad física, psicológica o sexual de los menores de edad.

6.3. Configurar perfiles para niños y adolescentes, activar controles parentales y opciones de privacidad por defecto en los sistemas operativos, aplicaciones y plataformas utilizadas, y preferentemente utilizar alguna de las herramientas disponibles en el módulo "Modo Aprendizaje", de manera voluntaria y conforme a sus necesidades.

6.4. Cuando el dispositivo cuente con servicio público de telecomunicaciones, solicitar a la empresa operadora, a través de canales gratuitos, la activación, actualización, suspensión o revocación del marcador de estado en el RDU-NA, con atención en el plazo establecido en el reglamento.

6.5. Cuando el servicio de telecomunicaciones o el dispositivo asociado vaya a ser utilizado habitualmente por un niño o adolescente, el titular de la línea debe declararlo ante la empresa operadora, otorgando su consentimiento verificable para la activación del marcador de estado y para la aplicación de configuraciones protectoras por defecto.

6.6. Cuando el servicio o el dispositivo asociado deje de ser utilizado habitualmente por un niño o adolescente, o cuando la persona usuaria alcance la mayoría de edad, el titular deberá comunicar dicha situación a la empresa operadora y solicitar la actualización o variación de la declaración respectiva.

6.7. Las orientaciones previstas en el presente artículo forman parte de la corresponsabilidad familiar en la protección de los menores de edad y no constituyen, por sí mismas, infracciones administrativas ni generan un régimen sancionador especial, sin perjuicio de las responsabilidades establecidas en la legislación vigente.

CAPÍTULO III

OBLIGACIONES DE OPERADORAS Y PROVEEDORES

Artículo 7. Obligación de las empresas operadoras de servicios públicos de telecomunicaciones

7.1. Las empresas operadoras de servicios públicos de telecomunicaciones, antes de la contratación o activación del servicio, tienen las siguientes obligaciones:

a) Informar al usuario, de manera clara, accesible y gratuita, sobre el Registro de Dispositivos Móviles de Uso por Niños y Adolescentes (RDU-NA), el marcador de estado «dispositivo utilizado por un menor de edad», su finalidad y los efectos de las configuraciones de protección correspondientes, precisando que su implementación no autoriza la inspección del contenido de las comunicaciones privadas.

b) Consultar al usuario si la línea o el dispositivo asociado será utilizado habitualmente por un menor de edad e informarle sobre el procedimiento de declaración y activación del marcador de estado.

c) Cuando se declare el uso habitual por un menor de edad, recabar el consentimiento verificable del padre, madre o tutor para la activación del marcador de estado en el RDU-NA y la aplicación de las configuraciones de protección correspondientes, sin incorporar datos de identidad del menor de edad al registro y conforme a la normativa de protección de datos personales.

d) Facilitar al titular del servicio la configuración de medidas de protección para las líneas celulares declaradas de uso habitual por menores de edad, considerando los grupos etarios, las recomendaciones de uso y las reglas de acceso y control establecidas en el artículo 5 de la presente ley. Estas medidas comprenden, según la disponibilidad y compatibilidad técnica del dispositivo móvil, el servicio y la plataforma digital, controles parentales, perfiles de protección, límites de tiempo de uso y herramientas de privacidad

y seguridad, sin que ello implique restricciones automáticas al servicio de telefonía, mensajería o acceso a internet.

e) Proporcionar información y asistencia gratuita para la instalación y configuración de las herramientas disponibles en el módulo «Modo Aprendizaje», así como orientación para verificar su funcionamiento, de acuerdo con la compatibilidad del dispositivo, sistema operativo o servicio utilizado.

f) Emitir una constancia al representante y activar el marcador de estado en el RDU-NA, con fecha de expiración automática.

g) Implementar canales gratuitos y accesibles para activar, renovar, suspender o revocar el marcador de estado, con ejecución en un máximo de diez días hábiles.

h) Desactivar el marcador de estado cuando ocurra el cambio de titularidad de la línea, la portabilidad a otra empresa, la transferencia del equipo, la baja de la línea o el vencimiento del plazo del marcador. En todos los casos, el usuario puede solicitar su reactivación.

i) No condicionar la venta o la calidad del servicio a la activación del marcador de estado ni cobrar por activarlo o desactivarlo.

7.2. Las empresas operadoras informan, de manera clara, destacada y verificable, antes de establecer la relación contractual con el usuario y cada seis meses mientras esta dure, sobre la disponibilidad, alcance, costo y forma de activación y desactivación, a solicitud del abonado, de los controles parentales o filtros de contenido orientados a la protección de menores de edad en los servicios fijos y móviles. Esta información consta en el contrato y en los canales de atención. Los medios empleados para publicitar la disponibilidad de los controles parentales y filtros son similares a los utilizados por las empresas operadoras para promocionar sus servicios.

7.3. Las empresas operadoras facilitan y ponen a disposición de sus usuarios herramientas o mecanismos de control parental que, como mínimo y a solicitud del abonado, permitan la activación de perfiles de protección para menores de edad, la limitación por horarios y tiempo de uso y el filtrado por categorías de contenido de alto riesgo, conforme al reglamento de la presente ley y a las características técnicas del servicio o dispositivo. Asimismo, pueden ofrecer opciones adicionales, gratuitas u onerosas, según su oferta comercial.

7.4. El uso de controles parentales o filtros se realiza exclusivamente a solicitud del abonado, no implica bloqueos ni degradaciones injustificadas del servicio y no afecta la neutralidad de la red. Su implementación se sujeta a la normativa de telecomunicaciones, protección al consumidor y protección de datos personales.

7.5. Las empresas operadoras que comercialicen dispositivos móviles incluyen mensajes preventivos sobre los riesgos para la salud mental y el bienestar digital de menores de edad en los puntos de venta y materiales publicitarios. Los mensajes se publican mediante etiquetas con advertencias estandarizadas, aprobadas por el Ministerio de Salud. Estos mensajes tienen carácter informativo y no limitan la comercialización de los dispositivos móviles.

Asimismo, los proveedores de sistemas operativos de dispositivos móviles destinados al uso de menores de edad incorporan advertencias claras y visibles sobre los riesgos

asociados al uso excesivo, la exposición a contenidos no supervisados y sus implicancias para la salud física y mental.

La elaboración, difusión, fiscalización y sanción de dichos mensajes se rigen por la Ley 29571, Código de Protección y Defensa del Consumidor, y por el Decreto Legislativo 1044, Decreto Legislativo que aprueba la Ley de Represión de la Competencia Desleal, en el ámbito de las competencias del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

Artículo 8. Obligación de los proveedores de servicios digitales

8.1. Los proveedores de servicios digitales, incluidas las plataformas de redes sociales, videojuegos en línea y otros servicios digitales ofrecidos o disponibles en el mercado peruano, adoptan medidas de protección reforzada para los usuarios menores de edad, considerando la naturaleza del servicio, los riesgos asociados a su utilización, la edad y el grado de madurez de sus usuarios.

8.2. Los proveedores de servicios digitales implementan, en el ámbito de sus funcionalidades y de manera proporcional a los riesgos identificados, las siguientes medidas:

a) Establecer configuraciones de privacidad y seguridad por defecto para las cuentas identificadas como pertenecientes a menores de edad, limitando la exposición pública de información personal y la posibilidad de contacto no solicitado por usuarios desconocidos.

b) Proporcionar herramientas accesibles para gestionar el tiempo de uso, establecer periodos de descanso y desactivar notificaciones no esenciales, así como mecanismos que permitan limitar funcionalidades de uso continuado, tales como la reproducción automática de contenidos y el desplazamiento infinito.

c) Implementar mecanismos accesibles para denunciar situaciones de ciberacoso, captación con fines sexuales, sextorsión, amenazas y otras formas de violencia digital, así como procedimientos para su evaluación y atención oportuna, de conformidad con la normativa vigente.

d) Facilitar herramientas de supervisión y acompañamiento parental, adecuadas a la edad y grado de madurez de los menores de edad, que respeten su privacidad, autonomía progresiva y derecho a la confidencialidad de las comunicaciones.

e) Proporcionar información clara, comprensible y accesible sobre las condiciones de uso del servicio, sus principales riesgos, las medidas de protección disponibles y los canales de orientación y asistencia.

f) Abstenerse de utilizar datos personales de menores de edad para elaborar perfiles destinados a publicidad comportamental, así como de emplear mecanismos de diseño que induzcan deliberadamente a

proporcionar datos personales innecesarios o a desactivar las configuraciones de protección.

8.3. Los proveedores de servicios digitales adoptan mecanismos de verificación o aseguramiento de la edad adecuados a la naturaleza y riesgos del servicio, de conformidad con la Ley 29733, Ley de Protección de Datos Personales, y su reglamento. Dichos mecanismos deben observar los principios de proporcionalidad, finalidad, seguridad y minimización de datos personales, evitando la recopilación o conservación injustificada de información biométrica o documentos de identidad.

8.4. Las medidas previstas en el presente artículo no autorizan la inspección indiscriminada de comunicaciones privadas, la vigilancia generalizada de los usuarios ni el tratamiento de datos personales incompatible con las finalidades de protección establecidas en la presente ley.

8.5. El reglamento establece los criterios técnicos para la aplicación progresiva y proporcional de las medidas previstas en el presente artículo, considerando la naturaleza de los servicios digitales, sus funcionalidades, los riesgos para los menores de edad y las condiciones de accesibilidad, sin establecer obligaciones que impliquen la vulneración de derechos fundamentales.

8.6. Los proveedores de servicios digitales facilitan, cuando resulte técnicamente viable y conforme a los estándares establecidos en el reglamento, la compatibilidad de sus herramientas de protección con las configuraciones asociadas al marcador de estado «dispositivo utilizado por un menor de edad» y con el módulo «Modo Aprendizaje», a fin de favorecer la aplicación de medidas de privacidad, seguridad y acompañamiento parental adecuadas al grupo etario correspondiente. Los proveedores de servicios digitales deben diseñar sus servicios aplicando el principio de seguridad y privacidad por diseño (*safety and privacy by design*), de manera que las configuraciones protectoras para menores sean las predeterminadas y no requieran acción adicional del usuario para activarse.

La implementación de estos mecanismos no autoriza el acceso directo e indiscriminado al Registro de Dispositivos Móviles de Uso por Niños y Adolescentes (RDU-NA), la identificación del menor de edad ni el tratamiento de datos personales para finalidades distintas de las previstas en la presente ley.

<u>Artículo 9.</u> Registro de dispositivos móviles de uso por niños y adolescentes (RDU-NA)

9.1. Se crea el Registro de Dispositivos Móviles de Uso por Niños y Adolescentes (RDU-NA), con la finalidad exclusiva de facilitar la aplicación de configuraciones de privacidad y seguridad por defecto, herramientas de protección digital y mecanismos de control parental en los dispositivos móviles y servicios públicos de telecomunicaciones declarados para uso habitual por menores de edad, conforme al principio del interés superior del niño.

El RDU-NA no constituye un mecanismo de vigilancia ni autoriza la inspección de comunicaciones privadas, el seguimiento de la navegación, la recopilación de datos de tráfico o el filtrado indiscriminado de contenidos.

9.2. La Autoridad Nacional de Protección de Datos Personales (ANPD) tiene a su cargo la administración del RDU-NA y la supervisión del tratamiento de datos personales asociado a su funcionamiento, conforme a las competencias establecidas en la presente ley y en la normativa de protección de datos personales.

Las empresas operadoras de servicios públicos de telecomunicaciones ejecutan los procedimientos de activación, actualización, suspensión y revocación del marcador de estado, de acuerdo con las condiciones técnicas y operativas establecidas en el reglamento, sin perjuicio de las competencias del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

9.3. El RDU-NA contiene exclusivamente la siguiente información:

a) El marcador de estado «dispositivo utilizado por un menor de edad».
b) La fecha de activación y la fecha de expiración del marcador.
c) El grupo etario o perfil de protección aplicable, sin consignar la edad exacta del menor de edad.
d) La constancia seudonimizada de la obtención del consentimiento verificable del padre, madre o tutor.
e) Un identificador técnico seudonimizado, estrictamente necesario para la gestión del marcador de estado.

La información registrada se limita a los datos indispensables para las finalidades previstas en la presente ley.

9.4. Queda prohibido incorporar al RDU-NA nombres, documentos de identidad, números telefónicos, fechas de nacimiento, datos de geolocalización, registros de navegación, datos de tráfico, contenido de comunicaciones privadas o cualquier otro dato que permita identificar directamente al menor de edad o a su representante.

Las empresas operadoras mantienen separada la información contractual y la evidencia necesaria para acreditar el consentimiento verificable respecto de la información incorporada al RDU-NA. Dicha información se conserva únicamente durante el plazo necesario para cumplir las finalidades legítimas correspondientes y las obligaciones establecidas en la normativa vigente.

9.5. La activación del marcador de estado requiere la declaración del uso habitual del dispositivo o servicio por un menor de edad y el consentimiento verificable del padre, madre o tutor, conforme a los artículos 6 y 7 de la presente ley.

La empresa operadora determina la fecha de expiración del marcador sobre la base de la información proporcionada para establecer el grupo etario correspondiente, sin incorporar al RDU-NA la fecha de nacimiento ni los datos de identidad del menor de edad.

El marcador expira automáticamente cuando el usuario alcanza la mayoría de edad, sin perjuicio de las actualizaciones, suspensiones o revocaciones anticipadas que correspondan. La revisión periódica de las condiciones de protección no modifica dicha fecha de expiración, salvo que resulte necesario corregirla por información debidamente actualizada.

9.6. El titular del servicio público de telecomunicaciones, con intervención del padre, madre o tutor cuando corresponda, puede solicitar en cualquier momento la activación, renovación, actualización, suspensión o revocación del marcador de estado, mediante canales gratuitos y accesibles.

Las empresas operadoras atienden dichas solicitudes dentro del plazo máximo establecido en el artículo 7 de la presente ley y proporcionan información clara sobre los efectos de la modificación solicitada.

9.7. Se prohíbe utilizar el RDU-NA, el marcador de estado o la información obtenida mediante su implementación para fines, comerciales, elaboración de perfiles publicitarios, publicidad comportamental, fijación diferenciada de precios, segmentación comercial de usuarios, vigilancia generalizada o cualquier otra finalidad ajena a la protección digital de menores de edad prevista en la presente ley.

Asimismo, se prohíbe correlacionar la información del registro con datos de geolocalización, tráfico, navegación o contenido de comunicaciones privadas.

9.8. El padre, madre o tutor, a través del titular del servicio cuando corresponda, puede solicitar la desactivación del marcador de estado y la supresión de los datos asociados al RDU-NA, conforme a la normativa de protección de datos personales.

Cuando se produzca el cambio de titularidad de la línea, la portabilidad a otra empresa operadora, la transferencia del dispositivo, la baja del servicio o cualquier otra circunstancia que determine la pérdida de las condiciones que justificaron la activación del marcador, la empresa operadora efectúa la actualización o desactivación correspondiente, de conformidad con el artículo 7 de la presente ley.

La información que deje de ser necesaria para la finalidad del registro es suprimida o anonimizada, sin perjuicio de los plazos de conservación legalmente exigibles.

La desactivación del marcador no afecta la continuidad ni la calidad del servicio contratado.

9.9. La administración y funcionamiento del RDU-NA se sujetan a las disposiciones de la Ley 29733, Ley de Protección de Datos Personales, y su reglamento, así como a las medidas de seguridad y confidencialidad que resulten aplicables.

Previamente a su implementación se realiza una evaluación de impacto en la protección de datos personales, destinada a identificar y mitigar los riesgos asociados al tratamiento de información y al funcionamiento del registro.

La evaluación se actualiza cuando se introduzcan modificaciones sustanciales que puedan incrementar los riesgos para los derechos de los titulares de datos personales.

9.10. Las empresas operadoras de servicios públicos de telecomunicaciones adoptan las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y seguridad de la información tratada para la gestión del marcador de estado.

El tratamiento de dicha información se realiza conforme a los principios de finalidad, proporcionalidad y seguridad previstos en la normativa de protección de datos personales, limitándose a la gestión de las solicitudes de los titulares, la ejecución de las medidas de protección autorizadas y la acreditación del cumplimiento de las obligaciones establecidas en la presente ley.

9.11. El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) supervisa, en el ámbito de sus competencias, el cumplimiento de las obligaciones de las empresas operadoras relativas a la información, disponibilidad y gestión del marcador de estado, así como a la prestación de las funcionalidades de protección previstas en la presente ley.

La ANPD ejerce sus competencias de supervisión y fiscalización respecto del tratamiento de datos personales asociado al RDU-NA, sin perjuicio de las atribuciones del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) en materia de protección al consumidor y publicidad comercial.

9.12. El reglamento establece las condiciones técnicas y operativas para el funcionamiento del RDU-NA, los procedimientos de consentimiento verificable, los mecanismos de seudonimización, las condiciones de interoperabilidad, los procedimientos de activación, renovación, actualización, suspensión y revocación del marcador de estado, así como las medidas necesarias para garantizar su expiración automática.

La implementación de dichos mecanismos respeta la normativa de protección de datos personales, la confidencialidad de las comunicaciones y el principio de neutralidad de red.

9.13. El reglamento establece un mecanismo de revisión periódica del funcionamiento del RDU-NA, como máximo a los tres años de su implementación, con el fin de evaluar su efectividad, los riesgos residuales para la protección de datos personales y la pertinencia de mantener o modificar el registro. Dicha revisión se realiza con participación de la ANPD, OSIPTEL y la Comisión Multisectorial prevista en la presente ley.

CAPÍTULO IV

PROTECCIÓN EN ESPACIOS CON ACCESO PÚBLICO A INTERNET

Artículo 10. Protección de niños y adolescentes en lugares con acceso público a internet

10.1. Los establecimientos, sean públicos o privados, que brinden servicio de acceso a internet al público en general deben implementar filtros mínimos que impidan el acceso a contenidos manifiestamente perjudiciales para niños y adolescentes, en particular aquellos de carácter pornográfico, de violencia extrema o de apuestas en línea, cuando ofrezcan los siguientes servicios:

a) Alquiler de cabinas públicas de internet.

b) Internet gratuito o rentado para clientes en restaurantes, hoteles, aeropuertos, centros comerciales u otros similares.

c) Internet gratuito o rentado en plazas, parques, instalaciones gubernamentales de cualquier clase u otros similares.

10.2. Los establecimientos implementan mecanismos de protección adecuados a la naturaleza del servicio, incluyendo, cuando resulte técnicamente viable, configuraciones de navegación segura e información visible sobre el uso seguro y responsable de internet.

10.3. Los establecimientos informan de manera visible, en carteles o en su página web, sobre la existencia de filtros de contenido y las recomendaciones de uso seguro, e incluyen una política de uso aceptable y un enlace a recursos públicos de bienestar digital.

10.4. Las municipalidades distritales y provinciales, de acuerdo con sus atribuciones, establecen e imponen sanciones por infracciones a lo dispuesto en los párrafos anteriores. El reglamento de la presente ley especifica las infracciones y las sanciones según la gravedad de cada hecho.

CAPÍTULO V

ACCIONES SECTORIALES

Artículo 11. Acciones a cargo del Ministerio de Educación

11.1. El Ministerio de Educación (MINEDU), en el marco de sus competencias, promueve la incorporación y el fortalecimiento de contenidos y competencias relacionados con la ciudadanía digital, la seguridad en internet, el bienestar digital y el uso responsable de las tecnologías en el Currículo Nacional de la Educación Básica, así como en los materiales y recursos pedagógicos correspondientes.

11.2. El MINEDU, en coordinación con las direcciones regionales de educación y las unidades de gestión educativa local, promueve acciones de formación continua y fortalecimiento de capacidades dirigidas a docentes, directivos y demás integrantes de la comunidad educativa, orientadas a:

a) Prevenir e identificar oportunamente situaciones de ciberacoso, violencia digital, captación con fines sexuales y exposición a contenidos perjudiciales para niños y adolescentes.
b) Promover hábitos saludables de utilización de dispositivos móviles y servicios digitales, considerando sus efectos en el aprendizaje, el descanso, la convivencia escolar y el bienestar socioemocional.
c) Fortalecer las competencias para el uso pedagógico, seguro y responsable de las tecnologías digitales.

11.3. El MINEDU, en el ámbito de sus competencias, establece las disposiciones y orientaciones correspondientes al uso de dispositivos móviles en las instituciones educativas de educación básica, de conformidad con la Ley 32385 y su reglamento, considerando las necesidades pedagógicas, las condiciones de accesibilidad, la inclusión educativa y la protección integral de los estudiantes.

11.4. El MINEDU, en coordinación con el Ministerio de Salud (MINSA) y el Ministerio de la Mujer y Poblaciones Vulnerables (MIMP), promueve la implementación de mecanismos de identificación temprana, orientación y derivación oportuna de estudiantes que presenten señales de afectación de su bienestar socioemocional o se encuentren expuestos a situaciones de riesgo asociadas al uso de entornos digitales.

Estas acciones se desarrollan mediante los protocolos y mecanismos de atención existentes, procurando su articulación con los servicios especializados de salud y protección que correspondan, y garantizando la confidencialidad de la información, la protección de datos personales y el interés superior del niño.

11.5. El MINEDU, a través de las instancias de gestión educativa descentralizada, promueve estrategias de participación y orientación dirigidas a padres, madres y tutores, con la finalidad de fortalecer el acompañamiento familiar, la prevención de riesgos digitales, el establecimiento de límites razonables de tiempo de uso y la utilización de herramientas de control parental y protección digital, respetando la autonomía progresiva de niños y adolescentes.

11.6. El MINEDU promueve que las instituciones educativas incorporen acciones de prevención de la violencia digital y promoción del bienestar digital en sus instrumentos de gestión y actividades de convivencia escolar, de conformidad con la normativa vigente, evitando la duplicidad de mecanismos de atención, seguimiento y reporte.

11.7. El MINEDU, en coordinación con las entidades competentes, establece indicadores de seguimiento de las acciones educativas desarrolladas en aplicación de la presente ley y proporciona información estadística consolidada a la comisión multisectorial prevista en el artículo 14 de la presente ley, para la evaluación de sus resultados y la elaboración de los informes correspondientes.

La información proporcionada respeta la confidencialidad de los estudiantes y la normativa de protección de datos personales.

Artículo 12. Acciones a cargo del Ministerio de Salud

12.1. El Ministerio de Salud (MINSA), en el marco de sus competencias, desarrolla y promueve acciones de información, educación y comunicación orientadas a prevenir los riesgos psicosociales asociados al uso temprano, intensivo o problemático de dispositivos móviles, plataformas y servicios digitales por niños y adolescentes, considerando su edad, grado de madurez y condiciones de vulnerabilidad, con enfoque preventivo, intercultural, inclusivo y accesible.

12.2. El MINSA elabora, aprueba y actualiza, conforme a la evidencia científica disponible, guías y documentos técnicos para la identificación temprana, evaluación, orientación, intervención y derivación oportuna de niños y adolescentes que presenten problemas de salud mental asociados al uso problemático de tecnologías y servicios digitales.

Dichos instrumentos orientan la actuación del personal de salud, especialmente en el primer nivel de atención y en los centros de salud mental comunitaria, de conformidad con las competencias de cada establecimiento y los mecanismos de referencia y contrarreferencia correspondientes, garantizando la confidencialidad de la información y la protección de datos personales.

12.3. El MINSA, mediante los servicios y canales de atención disponibles, fortalece las acciones de orientación y teleorientación dirigidas a niños, adolescentes y sus familias sobre bienestar digital, identificación de señales de alerta y prevención de riesgos para la salud mental.

Asimismo, promueve la derivación oportuna a los servicios de salud mental que correspondan, en coordinación con el Ministerio de Educación y el Ministerio de la Mujer y Poblaciones Vulnerables, conforme a sus respectivas competencias.

12.4. El MINSA promueve acciones de capacitación y actualización continuada, dirigidas al personal de salud sobre bienestar digital, identificación temprana de riesgos psicosociales, orientación familiar, intervenciones preventivas y derivación oportuna de niños y adolescentes que presenten señales de afectación de su salud mental vinculadas al uso problemático de tecnologías digitales.

Para tal efecto, puede articular acciones de cooperación académica y técnica con universidades, colegios profesionales y otras instituciones especializadas, de conformidad con la normativa vigente.

12.5. El MINSA, en coordinación con las entidades competentes, desarrolla mecanismos de seguimiento de indicadores relacionados con la salud mental y el bienestar digital de niños y adolescentes, utilizando información estadística y evidencia disponible que permita identificar tendencias, factores de riesgo y necesidades de intervención.

Asimismo, elabora un reporte anual sobre la situación y las acciones desarrolladas en esta materia, el cual se publica en su portal institucional y se remite a la

comisión multisectorial prevista en el artículo 14 de la presente ley, para su incorporación en el informe anual dirigido al Congreso de la República.

La información difundida tiene carácter agregado y anonimizado, en observancia de la Ley 29733, Ley de Protección de Datos Personales, y su reglamento.

12.6. El MINSA elabora, aprueba y actualiza una guía técnica de recomendaciones y advertencias sanitarias sobre los posibles efectos del uso temprano, intensivo o problemático de dispositivos móviles y servicios digitales en la salud física y mental de niños y adolescentes, diferenciando las orientaciones según los grupos etarios y la evidencia científica disponible.

La guía contiene, como mínimo, recomendaciones sobre tiempo de exposición a pantallas, higiene del sueño, pausas activas, actividad física, acompañamiento familiar, identificación de señales de alerta y acceso oportuno a servicios de orientación y atención en salud mental.

Asimismo, comprende mensajes de prevención y advertencias sanitarias para su difusión en campañas públicas, materiales educativos y demás mecanismos de información previstos en la presente ley, en coordinación con los sectores competentes.

Artículo 13. Acciones a cargo del Ministerio de la Mujer y Poblaciones Vulnerables

13.1. El Ministerio de la Mujer y Poblaciones Vulnerables (MIMP), en el marco de sus competencias, promueve y desarrolla acciones de prevención, orientación y protección de niños y adolescentes frente a los riesgos y situaciones de violencia asociados al uso de entornos digitales, con especial atención a aquellos que puedan afectar su salud mental, integridad física y psicológica, seguridad y desarrollo integral, priorizando a quienes se encuentran en situación de vulnerabilidad.

13.2. El MIMP, en coordinación con el Ministerio de Educación, el Ministerio de Salud y las demás entidades competentes, promueve programas y acciones de orientación y acompañamiento dirigidos a padres, madres, tutores y responsables del cuidado de niños y adolescentes, destinados a fortalecer las competencias parentales, la comunicación familiar, la supervisión responsable y la identificación temprana de situaciones de riesgo en entornos digitales.

Estas acciones consideran la edad, el grado de madurez y la autonomía progresiva de los menores de edad, promoviendo prácticas de acompañamiento respetuosas de sus derechos.

13.3. El MIMP, a través de sus servicios y mecanismos de atención, conforme a sus competencias, facilita la orientación, atención y derivación oportuna de niños y adolescentes afectados por situaciones de violencia digital, incluyendo el ciberacoso, la captación con fines sexuales, la sextorsión, la difusión no

consentida de imágenes íntimas y otras conductas que comprometan su integridad física, psicológica o sexual.

Para tal efecto, articula su intervención con los servicios de salud, educación, protección y las autoridades competentes, según corresponda, procurando evitar la revictimización y garantizando una atención oportuna, accesible y adecuada a las necesidades de cada caso.

13.4. El MIMP promueve la elaboración y difusión de materiales informativos, campañas de sensibilización y pautas de orientación familiar sobre el uso seguro, responsable y equilibrado de las tecnologías digitales, la prevención de la violencia en línea, la protección de la privacidad y el reconocimiento de señales de alerta que puedan comprometer el bienestar de niños y adolescentes.

Dichos materiales consideran las necesidades de protección según los grupos etarios, las condiciones de accesibilidad, la pertinencia cultural y lingüística y las circunstancias de especial vulnerabilidad.

13.5. Las acciones previstas en el presente artículo se desarrollan con observancia del principio del interés superior del niño, la autonomía progresiva, el respeto de la dignidad, la confidencialidad de la información y la protección de datos personales, de conformidad con la legislación vigente.

Asimismo, el MIMP proporciona a la comisión multisectorial, prevista en el artículo 14 de la presente ley, información estadística consolidada sobre las acciones desarrolladas y sus resultados, para contribuir al seguimiento y evaluación de las medidas de protección, sin revelar información que permita identificar a los niños y adolescentes atendidos.

CAPÍTULO VI

GOBERNANZA Y COORDINACIÓN

Artículo 14. Articulación intersectorial para la protección de la salud mental de menores de edad en entornos digitales

14.1. La Presidencia del Consejo de Ministros (PCM), en el marco de sus competencias y de conformidad con la normativa que regula la organización y funcionamiento del Poder Ejecutivo, promueve la constitución de una comisión multisectorial de naturaleza permanente, encargada de articular, coordinar y efectuar el seguimiento de las acciones destinadas a promover el uso seguro, responsable y saludable de las tecnologías digitales, así como la protección de la salud mental y el bienestar digital de niños y adolescentes.

La constitución y funcionamiento de dicha comisión se sujetan a las disposiciones aplicables a las comisiones multisectoriales del Poder Ejecutivo.

14.2. La comisión multisectorial tiene las siguientes funciones:

a) Proponer lineamientos y recomendaciones para la articulación de las acciones de prevención, educación, orientación, protección y promoción

del bienestar digital de niños y adolescentes, respetando las competencias de las entidades involucradas.

b) Coordinar la elaboración y el seguimiento de planes anuales de trabajo intersectorial, considerando las acciones desarrolladas por el Ministerio de Educación, el Ministerio de Salud, el Ministerio de la Mujer y Poblaciones Vulnerables y las demás entidades competentes.
c) Promover campañas nacionales de información y sensibilización sobre los riesgos asociados al uso problemático de tecnologías digitales, la prevención de la violencia digital y el fortalecimiento del acompañamiento familiar.
d) Promover mecanismos de cooperación con las empresas operadoras de servicios públicos de telecomunicaciones, los proveedores de plataformas y servicios digitales, las instituciones educativas, las universidades y las organizaciones de la sociedad civil, de conformidad con la normativa vigente.
e) Articular la recopilación y sistematización de información estadística e indicadores sobre las acciones desarrolladas por las entidades participantes, garantizando la confidencialidad y la protección de datos personales.
f) Formular recomendaciones para mejorar la eficacia de las medidas de protección previstas en la presente ley, sobre la base de la evidencia científica disponible, los resultados de su implementación y las necesidades identificadas en la población infantil y adolescente.

14.3. La comisión multisectorial no ejerce funciones de regulación sectorial, supervisión, fiscalización ni sanción, las cuales corresponden a las entidades competentes conforme al ordenamiento jurídico vigente.

Sus acuerdos y recomendaciones se desarrollan respetando las atribuciones de las entidades que la integran y no sustituyen los procedimientos ni las decisiones que corresponden a cada autoridad.

14.4. La Presidencia del Consejo de Ministros remite anualmente al Congreso de la República, a más tardar el último día hábil de marzo, un informe sobre las acciones desarrolladas durante el año calendario anterior, los resultados obtenidos, las dificultades identificadas y las recomendaciones formuladas para fortalecer la protección de la salud mental y el bienestar digital de niños y adolescentes.
El informe se publica en el portal institucional de la Presidencia del Consejo de Ministros dentro de los cinco días hábiles siguientes a su remisión y comprende información estadística consolidada proporcionada por las entidades competentes, respetando la normativa de protección de datos personales.

14.5. La constitución, organización y funcionamiento de la comisión multisectorial se sujetan a las disposiciones aplicables de la Ley 29158, Ley Orgánica del Poder Ejecutivo, y a la normativa vigente sobre comisiones multisectoriales.

Su funcionamiento se desarrolla con cargo a los recursos institucionales de las entidades participantes, conforme a la disponibilidad presupuestaria y sin generar la creación de nuevos pliegos presupuestarios.

Artículo 15. Conformación de la comisión multisectorial

15.1. La comisión multisectorial a que se refiere el artículo 14 está integrada por representantes de las siguientes entidades:
a) Presidencia del Consejo de ministros (PCM), que ejerce la presidencia.
b) Ministerio de Educación (MINEDU).
c) Ministerio de Salud (MINSA).
d) Ministerio de la Mujer y Poblaciones Vulnerables (MIMP).
e) Ministerio de Transportes y Comunicaciones (MTC).
f) Ministerio del Interior (MININTER).
g) Ministerio de Justicia y Derechos Humanos (MINJUSDH), a través de la Autoridad Nacional de Protección de Datos Personales (ANPD).
h) Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).
i) Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).
j) Un representante del sector privado
k) Un representante de la sociedad civil

15.2. La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de ministros, o la unidad orgánica que haga sus veces, ejerce la secretaría técnica de la comisión multisectorial, conforme a las disposiciones que regulen su constitución y funcionamiento.

15.3. Cada entidad integrante designa a un representante titular y a uno alterno, de conformidad con las disposiciones aplicables. La participación de los representantes es ad honórem y se desarrolla en el marco de las funciones institucionales correspondientes.

15.4. La Defensoría del Pueblo puede participar como invitada permanente, con voz y sin voto, respetando su autonomía constitucional.

15.5. La comisión multisectorial promueve la participación consultiva de representantes del sector privado, organizaciones de la sociedad civil, universidades, colegios profesionales y especialistas en salud mental, protección de menores de edad y derechos digitales, conforme a los mecanismos previstos en sus disposiciones de funcionamiento.

15.6. La comisión multisectorial puede convocar a representantes de gobiernos regionales, gobiernos locales y otras entidades públicas cuando los asuntos comprendidos en su agenda requieran coordinación territorial o especializada, respetando sus competencias y autonomía.

15.7. La organización y funcionamiento de la comisión multisectorial se sujetan a la normativa vigente y se financian con cargo a los presupuestos institucionales de las entidades participantes, sin demandar recursos adicionales al tesoro público.

Artículo 16. Participación del sector privado y de la sociedad civil

16.1. Las entidades públicas competentes, en coordinación con la comisión multisectorial prevista en el artículo 14 de la presente ley, promueven la

participación voluntaria del sector privado, las instituciones académicas, los colegios profesionales, las asociaciones de padres de familia de las instituciones educativas y otras organizaciones de la sociedad civil en acciones de información, prevención, educación y sensibilización destinadas a fomentar el uso seguro, responsable y saludable de las tecnologías digitales y la protección de la salud mental de menores de edad.

16.2. La participación comprende, entre otras, las siguientes acciones:
a) Colaborar en campañas de información y sensibilización sobre los riesgos asociados al uso problemático de tecnologías digitales, la prevención de la violencia digital y la promoción de hábitos saludables.
b) Promover la difusión de herramientas de control parental, configuraciones de privacidad y seguridad por defecto, recursos de bienestar digital y canales de orientación y asistencia dirigidos a menores de edad y sus familias.
c) Contribuir al desarrollo y difusión de materiales educativos, guías de orientación y actividades de capacitación dirigidas a padres, madres, tutores, docentes y demás personas responsables del cuidado y protección de menores de edad.
d) Impulsar actividades de investigación, intercambio de conocimientos y difusión de evidencia científica sobre los efectos del uso de tecnologías digitales en la salud mental y el desarrollo integral de menores de edad, conforme a la normativa vigente.

16.3. Las acciones de colaboración pueden desarrollarse mediante convenios de cooperación interinstitucional, actividades conjuntas, asistencia técnica y otros mecanismos permitidos por el ordenamiento jurídico. Pueden participar empresas operadoras de servicios públicos de telecomunicaciones, proveedores de plataformas y servicios digitales, desarrolladores de sistemas operativos, tiendas de aplicaciones, instituciones educativas privadas, universidades, colegios profesionales y organizaciones de la sociedad civil.

16.4. La participación del sector privado y de la sociedad civil se rige por los principios de voluntariedad, transparencia, integridad, publicidad y no exclusividad. Los mecanismos de cooperación no generan derechos de exclusividad, preferencias comerciales, ventajas competitivas indebidas ni autorizaciones para utilizar nombres, símbolos o imágenes institucionales con fines publicitarios sin la autorización correspondiente.

16.5. Las actividades desarrolladas en aplicación del presente artículo respetan la normativa de protección de datos personales y los derechos de menores de edad. La cooperación no autoriza la utilización de datos personales de menores de edad con fines comerciales, publicitarios o de elaboración de perfiles, ni el acceso a información confidencial fuera de los supuestos legalmente permitidos.

16.6. La colaboración voluntaria prevista en el presente artículo no sustituye ni limita el cumplimiento de las obligaciones legales de las empresas operadoras de servicios públicos de telecomunicaciones y de los proveedores de servicios digitales, ni modifica las competencias de supervisión y fiscalización de

OSIPTEL, INDECOPI y la Autoridad Nacional de Protección de Datos Personales, según corresponda.

16.7. Los costos derivados de las actividades de colaboración asumidas voluntariamente por las entidades privadas se financian con cargo a sus propios recursos. La participación de las entidades públicas se desarrolla conforme a sus competencias y disponibilidad presupuestal, sin generar asignaciones presupuestarias adicionales obligatorias.

Artículo 17. Herramientas de apoyo al control parental y al bienestar digital

17.1. La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, promueve e implementa el módulo denominado «Modo Aprendizaje», mediante herramientas, guías y recursos informativos gratuitos que faciliten a padres, madres y tutores la configuración de perfiles adecuados para menores de edad, el uso de controles parentales y la aplicación de opciones de privacidad y seguridad por defecto, aprovechando los canales y recursos digitales institucionales disponibles.

El módulo «Modo Aprendizaje» comprende:

a) Un catálogo oficial de referencia de herramientas de control parental y bienestar digital disponibles en el mercado, que incluya información sobre su compatibilidad con los principales sistemas operativos y plataformas digitales, así como sobre las funcionalidades para gestionar tiempos de uso, horarios, aplicaciones, permisos y restricciones de acceso a contenidos.
b) Guías, orientaciones técnicas, recomendaciones de configuración y recursos educativos destinados a promover el uso seguro, responsable y saludable de las tecnologías digitales por menores de edad.
c) Información técnica y criterios orientativos que permitan a las familias identificar y seleccionar herramientas de control parental y bienestar digital, considerando sus funcionalidades, condiciones de uso, medidas de privacidad y seguridad y adecuación a las necesidades de los menores de edad.

17.2. Las herramientas y recursos comprendidos en el módulo «Modo Aprendizaje» se desarrollan bajo los principios de privacidad y seguridad por defecto, minimización de datos personales, accesibilidad y facilidad de uso. Su utilización es voluntaria y no exclusiva, y las familias pueden elegir libremente entre las soluciones disponibles en el mercado.

La implementación de la iniciativa no exige el desarrollo de una aplicación estatal ni autoriza el tratamiento de datos personales fuera de los supuestos permitidos por la Ley 29733, Ley de Protección de Datos Personales, y su reglamento.

17.3. La PCM coordina con el Ministerio de Educación (MINEDU) y el Ministerio de Salud (MINSA) la incorporación de contenidos de ciudadanía y bienestar digital en las herramientas y guías de orientación. Asimismo, coordina con la Autoridad

Nacional de Protección de Datos Personales (ANPD), en el ámbito de sus competencias, la incorporación de recomendaciones y criterios técnicos para la protección de datos personales de menores de edad.

17.4. La PCM puede promover mecanismos de cooperación y suscribir convenios con tiendas de aplicaciones, proveedores de sistemas operativos y plataformas digitales para difundir el contenido del módulo «Modo Aprendizaje» y fomentar la disponibilidad de herramientas de control parental y configuraciones de privacidad y seguridad adecuadas para menores de edad, conforme a la normativa vigente.

CAPÍTULO VII

FISCALIZACIÓN Y SANCIONES

Artículo 18. Infracciones y sanciones relativas a empresas operadoras de servicios públicos de telecomunicaciones

18.1. El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) supervisa, fiscaliza y sanciona el incumplimiento de las obligaciones establecidas en la presente ley para las empresas operadoras de servicios públicos de telecomunicaciones.

18.2. Constituyen infracciones administrativas de las empresas operadoras:

a) Infracciones Leves:

1. No brindar la información periódica y semestral sobre controles parentales exigida en el numeral 7.2.
2. No entregar las constancias de activación o desactivación del marcador de estado en el RDU-NA.

b) Infracciones Graves:

3. No implementar los canales gratuitos para la activación, suspensión o revocación del marcador de estado conforme al numeral 7.1.
4. Condicionar la venta, la calidad del servicio o efectuar cobros por la activación o desactivación del marcador de estado.

c) Infracciones Muy Graves:

5. Incumplir con ejecutar la activación, suspensión o desactivación del marcador de estado en el RDU-NA dentro del plazo legal de diez (10) días hábiles.
6. Utilizar los datos del RDU-NA o del marcador de estado para fines comerciales, elaboración de perfiles o publicidad comportamental.

18.3. Las infracciones son sancionadas según la escala de multas establecida en la Ley 27336, Ley de desarrollo de las funciones y facultades del OSIPTEL

18.4. La responsabilidad de los proveedores es objetiva, en consecuencia, la carga de la prueba recae en el proveedor. Los proveedores de servicios de las Tecnologías de la Información (TICs) tendrán que demostrar que sus servicios se encuentran adaptados a la edad de los menores y que son seguros desde el diseño de estos.

18.5. La Autoridad Nacional de Protección de Datos Personales (ANPD), en el marco de las competencias conferidas por ley, ejerce su labor de supervisión, fiscalización y sanción respecto del tratamiento de datos personales de menores de edad. Asimismo, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus competencias legales, desarrolla sus acciones de fiscalización y sanción en materia de protección al consumidor y publicidad engañosa, de conformidad con la legislación vigente, sin perjuicio de las atribuciones de otras autoridades competentes.

18.6. El Ministerio de Transportes y Comunicaciones (MTC) ejerce las funciones que le corresponden conforme a su marco competencial establecido en la ley, sin perjuicio de las atribuciones de OSIPTEL.

En ningún caso procede la imposición de más de una sanción administrativa cuando exista identidad de sujeto, hecho y fundamento, conforme al principio de prohibición de doble sanción.

CAPÍTULO VIII

MEDIDAS COMPLEMENTARIAS DE PROTECCIÓN

Artículo 19. Protección de niños y adolescentes frente a la violencia en entornos digitales

19.1. El Estado, a través de las entidades competentes, promueve la prevención, detección temprana, atención y protección de niños y adolescentes frente a situaciones de violencia ejercida mediante tecnologías digitales, incluyendo el ciberacoso, la captación con fines sexuales, la sextorsión, la difusión no consentida de imágenes íntimas, las amenazas y otras conductas que puedan afectar su integridad física, psicológica o sexual.

19.2. El Ministerio de la Mujer y Poblaciones Vulnerables, en coordinación con el Ministerio de Educación, el Ministerio de Salud y las demás entidades competentes, promueve mecanismos de articulación para la orientación, atención psicológica, derivación y protección oportuna de niños y adolescentes afectados por situaciones de violencia en entornos digitales, de conformidad con la normativa vigente.

19.3. Las medidas de atención y protección consideran el interés superior del niño, su autonomía progresiva, la confidencialidad de la información y la participación de sus padres, tutores o responsables, siempre que dicha participación no comprometa su seguridad o bienestar.

19.4. La aplicación del presente artículo se realiza sin perjuicio de las medidas de protección, responsabilidades y procedimientos establecidos en la Ley 30364, el Código de los Niños y Adolescentes, el Código Penal y las demás disposiciones aplicables.

Artículo 20. Acciones contra la trata y explotación sexual en línea de niños y adolescentes

El Ministerio del Interior, el Ministerio de la Mujer y Poblaciones Vulnerables y las demás entidades competentes, en coordinación con los comités de seguridad ciudadana distritales y provinciales, proponen y ejecutan acciones concretas para la prevención y

lucha contra la trata y explotación sexual de niños y adolescentes en línea. El reglamento establece los plazos y mecanismos de articulación.

CAPÍTULO IX

FOMENTO, INVESTIGACIÓN Y COORDINACIÓN

Artículo 21. Promoción de la investigación sobre salud mental y bienestar digital de niños y adolescentes

21.1. El Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC), en coordinación con el Ministerio de Salud, promueve, en el marco de sus competencias, la investigación científica sobre los efectos del uso de tecnologías digitales, redes sociales, videojuegos y otros servicios digitales en la salud mental, el desarrollo cognitivo y el bienestar socioemocional de niños y adolescentes.

21.2. Las acciones de promoción de la investigación priorizan la generación de evidencia científica sobre los factores de riesgo y de protección asociados al uso de entornos digitales, la prevención de conductas de uso problemático, la identificación temprana de alteraciones de la salud mental y la evaluación de intervenciones preventivas y de acompañamiento familiar.

21.3. Las actividades de investigación pueden desarrollarse mediante los instrumentos y mecanismos de promoción y financiamiento de la investigación científica previstos en la normativa vigente, con participación de universidades, institutos de investigación y otras entidades competentes, conforme a sus respectivas atribuciones y disponibilidad presupuestal.

21.4. Los resultados de las investigaciones financiadas con recursos públicos se difunden de conformidad con la normativa aplicable, garantizando la protección de datos personales, la confidencialidad de la información de salud y los derechos de los niños y adolescentes participantes.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación

El Poder Ejecutivo, a través de la Presidencia del Consejo de ministros, aprueba el reglamento de la presente ley en un plazo no mayor de noventa días calendario contado a partir de su entrada en vigor.

SEGUNDA. Adecuación de normas

El Poder Ejecutivo, en el ámbito de sus competencias, adecúa las disposiciones reglamentarias que resulten necesarias para la aplicación de la presente ley, en un plazo no mayor de noventa días calendario contado a partir de su entrada en vigor, incluyendo, cuando corresponda:

a) El Reglamento de la Ley 29733, Ley de Protección de Datos Personales, aprobado por el Decreto Supremo 016-2024-JUS.

b) El Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por el Decreto Supremo 020-2007-MTC.

TERCERA. Plan de acción

La comisión multisectorial prevista en el artículo 14 de la presente ley presenta, en un plazo no mayor de ciento veinte días calendario contado a partir de su instalación, un Plan de acción orientado a la articulación y seguimiento de las medidas de prevención, educación, protección y promoción del bienestar digital establecidas en la presente ley.

CUARTA. Declaración de interés nacional

Se declara de interés nacional y de prioridad en las políticas públicas la protección de la salud mental y del desarrollo cognitivo, emocional y social de niños y adolescentes frente a los riesgos asociados al uso de las TIC y de los entornos digitales, así como la generación y puesta en marcha de políticas destinadas a informar, educar y sensibilizar sobre el uso seguro, responsable y saludable de dichos entornos, promoviendo la ciudadanía y el bienestar digital, y la prevención de riesgos psicosociales, conforme al interés superior del niño y al principio de autonomía progresiva.

QUINTA. Implementación de herramientas de apoyo al control parental y al bienestar digital

La Presidencia del Consejo de ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital o la unidad de organización que haga sus veces, establece, en un plazo no mayor de ciento veinte días calendario contado a partir de la entrada en vigor del reglamento de la presente ley, los criterios técnicos de funcionalidad, privacidad, seguridad y accesibilidad aplicables a las herramientas comprendidas en la iniciativa «Modo Aprendizaje», conforme al artículo 17.

La PCM pone a disposición de la ciudadanía, a través de los canales digitales institucionales, el catálogo de referencia, las guías de orientación y los recursos informativos gratuitos previstos en dicho artículo, sin que ello implique la obligación de desarrollar una aplicación estatal.

SEXTA. Implementación y financiamiento

La implementación de la presente Ley es progresiva y se financia con cargo al presupuesto institucional de las entidades involucradas, conforme a su disponibilidad presupuestaria y a las disposiciones del Sistema Nacional de Presupuesto Público, sin demandar recursos adicionales al Tesoro Público.

SÉPTIMA. Normas complementarias

Las entidades competentes de los tres niveles de gobierno dictan, en el ámbito de sus respectivas competencias y conforme al ordenamiento jurídico vigente, las disposiciones complementarias necesarias para la implementación de la presente ley.

OCTAVA. Período de adecuación

El Reglamento de la presente ley establece el periodo de adecuación y las fases de implementación para las entidades públicas, privadas y operadores obligados, considerando la naturaleza de las obligaciones, los recursos técnicos disponibles y el principio de gradualidad.

NOVENA. Evaluación de impacto y revisión de la ley

A los tres años de la entrada en vigor de la presente ley, la Comisión Multisectorial prevista en el artículo 14 elabora un informe de evaluación de impacto sobre la implementación de las medidas, su efectividad en la protección de la salud mental y el bienestar digital de niños y adolescentes, los costos de cumplimiento y los efectos no deseados. el informe se remite al Congreso de la República y se publica. Sobre la base de dicho informe, el Poder Ejecutivo puede proponer las modificaciones normativas que resulten necesarias.

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de los artículos 2, 5, 13, 16, 20 y 33 de la Ley 29733, Ley de Protección de Datos Personales

Se modifican los artículos 2, para incorporar el numeral 20; 5, para incorporar el segundo párrafo; 13, párrafo 13.3; 16, para incorporar un nuevo tercer párrafo; 20, para incorporar un nuevo cuarto párrafo y modificar la sumilla; y 33, numeral 6, de la Ley 29733, Ley de Protección de Datos Personales, en los siguientes términos:

"**Artículo 2. Definiciones**

Para todos los efectos de la presente Ley, se entiende por:

[…]

20. Protección de datos del niño y del adolescente. Conjunto de principios, derechos y garantías aplicables al tratamiento de datos personales de niños y adolescentes, incluyendo en entornos digitales. Se considera su interés superior y su derecho a la privacidad, en concordancia con el marco normativo nacional sobre protección de la infancia y de la adolescencia.

Artículo 5. Principio de consentimiento

[…]

El consentimiento para el tratamiento de datos personales del niño y del adolescente en entornos digitales debe garantizar que la recopilación, uso y difusión de su información cuenten con las autorizaciones correspondientes y los mecanismos efectivos de verificación, control parental y seguridad, conforme a lo establecido en el reglamento de la presente ley.

Artículo 13. Alcances sobre el tratamiento de datos personales

[…]

13.3. Mediante reglamento se dictan medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes, **con énfasis en su protección en entornos digitales y plataformas en línea**, así como para la protección y garantía de sus derechos. Para el ejercicio de los derechos que esta Ley reconoce, los niños y los adolescentes actúan a través de sus representantes legales, pudiendo el reglamento determinar las excepciones aplicables, de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente.

[…].

Artículo 16. Seguridad del tratamiento de datos personales

[…]

Para el tratamiento de datos personales del niño y del adolescente, el titular del banco de datos personales o el responsable de datos en plataformas o servicios en entornos digitales debe realizar esfuerzos razonables para verificar la edad de quienes otorguen su consentimiento, teniendo en cuenta la tecnología disponible.

Artículo 20. Derecho de actualización, inclusión, rectificación, supresión, y derecho al olvido digital en niños y adolescentes

[…]

En el caso del niño y del adolescente, el derecho de supresión incluye la eliminación de sus datos personales, cuando hayan sido publicados sin su consentimiento o sin el consentimiento del padre, madre o tutor, cuando dicha publicación represente un riesgo para su integridad, seguridad o privacidad. Los titulares de los datos personales, o sus representantes, deben ejercer estos derechos ante quienes hayan publicado el contenido reprochado, reclamado o cuestionado, objeto de la solicitud.

Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

[…]

6. Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes. **Asimismo, coordinar con el Ministerio de Educación y el Ministerio de la Mujer y Poblaciones Vulnerables la implementación de estrategias de educación y de concientización sobre la privacidad digital y la protección de datos personales de los niños y de los adolescentes que incluyan programas formativos para docentes, estudiantes y familias; campañas de sensibilización; y mecanismos de asistencia en casos de vulneración de la privacidad digital**.

[…]".

SEGUNDA. Modificación del artículo 4 de la Ley 27337, Código de los Niños y Adolescentes

Se modifica el primer párrafo del artículo 4 de la Ley 27337, Código de los Niños y Adolescentes, en los siguientes términos:

"**Artículo 4.- A su integridad personal.**

El niño y el adolescente tienen derecho a que se respete su integridad personal, física, psicológica, moral, psíquica y mental, **así como a la indemnidad y**

protección de su salud mental en los entornos digitales y servicios en línea. No podrán ser sometidos a tortura, ni a trato cruel o degradante. (…)"

TERCERA. Modificación del artículo 63 del Decreto Legislativo 702, que aprueba las normas que regulan la promoción de inversión privada en telecomunicaciones

Se modifica el artículo 63 del Decreto Legislativo 702, que aprueba las normas que regulan la promoción de inversión privada en telecomunicaciones, en los siguientes términos:

"**Artículo 63.** La utilización del espectro radioeléctrico dará lugar al pago de un canon que deberán satisfacer los titulares de estaciones radioeléctricas, emisoras y de las meramente receptoras que precisen de reserva radioeléctrica. El reglamento respectivo señalará los montos y formas de pago a propuesta del Ministerio de Transportes y Comunicaciones, los que serán aprobados mediante Decreto Supremo. **El Poder Ejecutivo queda facultado a priorizar, en un porcentaje no menor al 10% de los recursos recaudados por este concepto para el financiamiento de proyectos de investigación sobre trastornos asociados a la adicción a dispositivos móviles y servicios digitales en niños y adolescentes, bajo la coordinación del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica (CONCYTEC), conforme a las disposiciones y disponibilidad presupuestal que dicte dicho poder del Estado. […]".**

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogación

Se deroga la Ley 30254, Ley de promoción para el uso seguro y responsable de las tecnologías de la información y las comunicaciones por niños, niñas y adolescentes.

Lima, 04 de noviembre de 2026

FIRMA DIGITAL
Firmado digitalmente por: ROCHA GALLEGOS Roxana Maria FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 15:40:58-0500

FIRMA DIGITAL
Firmado digitalmente por: MARTINEZ PAITAN Paola Isabel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 04/11/2026 17:12:19-0500

FIRMA DIGITAL
Firmado digitalmente por: ROCHA GALLEGOS Roxana Maria FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 15:41:13-0500

FIRMA DIGITAL
Firmado digitalmente por: ARANDA VASQUEZ Christian FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 16:05:10-0500

FIRMA DIGITAL
Firmado digitalmente por: CIPRIANI THORNE Javier Jose Maria FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 16:23:37-0500

FIRMA DIGITAL
Firmado digitalmente por: YALTA SOTELO Carlos Alberto FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 17:23:03-0500

FIRMA DIGITAL
Firmado digitalmente por: KRKLEC TORRES Frank FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 16:42:10-0500

FIRMA DIGITAL
Firmado digitalmente por: BAELLA MALCA Jose Isidro FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/11/2026 17:39:28-0500

EXPOSICIÓN DE MOTIVOS

I. PLANTEAMIENTO DEL PROBLEMA PÚBLICO

I.1. Situación de la conectividad infantil y adolescente en el Perú del año 2026

La acelerada masificación de los entornos digitales representa una transformación estructural en el desarrollo de la niñez y la adolescencia en el Perú. De acuerdo con las cifras oficiales publicadas en setiembre del 2026 por el **Instituto Nacional de Estadística e Informática (INEI)**[1], en el segundo trimestre del 2026, "el 80,9% de los niños y adolescentes entre los 6 y 17 años de edad hizo uso del servicio de Internet. Entre la población de 6 a 11 años de edad, el acceso a Internet fue 68,2%, y entre la población de 12 a 17 años de edad alcanzó al 92,1%. Respecto al similar trimestre del año anterior, el uso del servicio de Internet se incrementó en la población de 6 a 11 años de edad (6,7 puntos porcentuales) y en la de 12 a 17 (2,3)."

Por otro lado, en el mismo segundo trimestre 2026, según otro informe del **INEI**[2] el 64,9% de la población de 6 a 17 años de edad usó este servicio a través de un teléfono celular, ya sea con o sin plan de datos. Otros dispositivos utilizados para conectarse a internet fueron la computadora (15,4%), la laptop (12,2%), la tablet (3,8%) y otros dispositivos, como los televisores inteligentes (smart TV), que alcanzaron una participación del 34,2%. Al comparar estos datos con el mismo trimestre de 2025, se observó un aumento de 4,0 puntos porcentuales en el uso del teléfono celular con o sin plan de datos, y 0,9 punto porcentual en el uso de la tablet para conectarse a Internet."

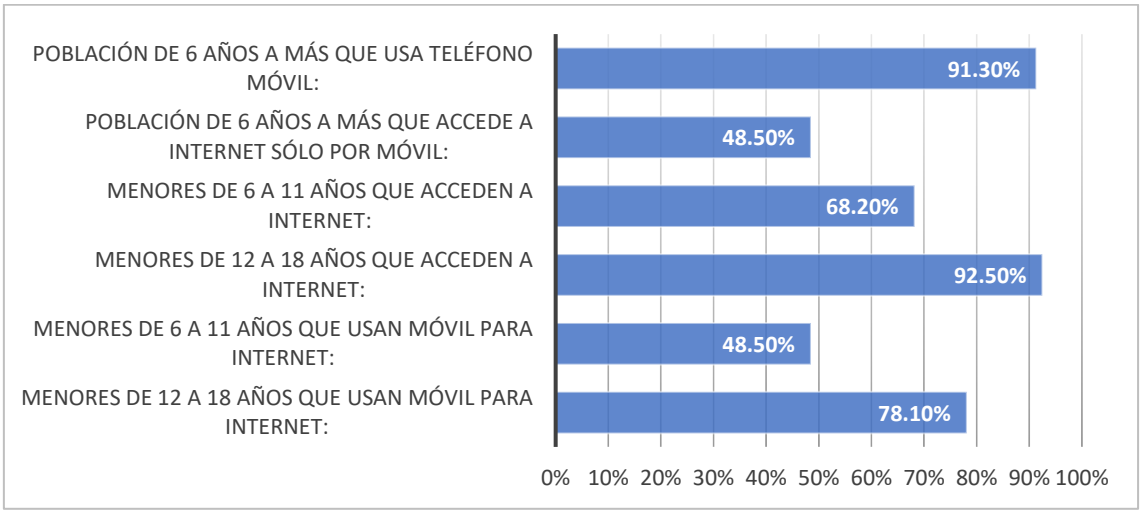
En cuanto al uso de internet en el ámbito territorial, también se han producido incrementos. Así tenemos que, en el segundo trimestre del año 2026, el 64,5% de los hogares del país accedió al servicio de internet. Esto muestra que, en el segundo trimestre del año 2026, el 64,5% de los hogares del país accedió al servicio de internet, mostrando una variación positiva de 3,8 puntos porcentuales respecto al mismo trimestre del año anterior (60,7%). De ello, se puede observar que el mayor crecimiento porcentual se dio en Lima Metropolitana en 4,3 puntos porcentuales (al pasar de 80,4% a 84,7%), seguido del resto urbano en 3,5 puntos porcentuales (de 62,7% a 66,2%) y el área rural, en 3,4 puntos porcentuales (al pasar de 23,7% a 27,1%)."

Esta alta exposición a entornos digitales sin mecanismos idóneos de supervisión o configuraciones de protección produce una situación de riesgo sistémico para cerca de 10 millones de niños y adolescentes (población de 0 a 17 años), quienes representan aproximadamente el 30% del conjunto nacional. Estos riesgos están asociados, de manera concreta, a riesgos de salud mental y adicción conductual, riesgos de explotación y seguridad personal, riesgos de desarrollo cognitivo y de socialización, riesgos en la privacidad del menor y su familia.

[1] Instituto Nacional de Estadística e Informática – Informe Técnico N°3. *"Estado de la Niñez y Adolescencia- II trimestre 2026"*, pp. 3 y 4. Disponible en: https://cdn.www.gob.pe/uploads/document/file/10591648/8576411-estado-de-la-ninez-y-adolescencia-ii-trimestre-2026.pdf?v=1788900953

[2] Instituto Nacional de Estadística e Informática- Informe Técnico Nº3, *"Estadísticas de las Tecnologías de Información y Comunicación en los Hogares"*. Disponible en: https://www.gob.pe/institucion/inei/noticias/1450362-el-64-5-de-los-hogares-del-pais-tiene-conexion-a-internet-durante-el-segundo-trimestre-de-2026

ACCESO Y USO DE DISPOSITIVOS MÓVILES (Segundo trimestre 2026)



Fuente: INEI (2026- II trimestre)

I.2. Impacto de los entornos digitales en la salud mental y la conducta de los niños y adolescentes

La exposición prolongada a entornos digitales altera el sistema de recompensa del cerebro de los menores -aún en desarrollo- mediante descargas constantes de dopamina generadas por los mecanismos de atracción-adicción que contiene la oferta de las plataformas digitales. Esto se traduce en conductas visibles y preocupantes:

a) Adicción a internet, adicción al celular y adicción a los videojuegos.

Las plataformas digitales están diseñadas para generar problemas de adicción en menores. Investigaciones del sector salud, realizadas por el Instituto Nacional de Salud Mental "Honorio Delgado - Hideyo Noguchi" (INSM "HD-HN"), señalan datos que ilustran la gravedad del problema relacionado con el uso excesivo de internet, celular y videojuegos. "Las niñas, niños y adolescentes peruanos pasan en promedio 35 horas semanales frente a una pantalla, superando ampliamente las 2 horas diarias recomendadas por la OMS."[3] Precisan que se ha observado "que en el nivel de severidad se alcanzó el 25% y, en un grado más moderado, el 40%. Esto quiere decir que uno de cada tres adolescentes en el Perú tiene problemas de uso excesivo de pantallas; ese es nuestro primer dato duro."[4]

b) **Afectación negativa de las redes sociales y plataformas digitales en la salud mental de los menores**.

Al respecto, una encuesta nacional realizada por **Aldeas Infantiles SOS Perú[5], en el primer semestre del 2025,** alerta sobre el impacto de los riesgos digitales en la salud

[3] Consejo Consultivo de Radio y Televisión – CONCORTV. Estudio sobre el Consumo y acceso de Niños, Niñas y Adolescentes a medios de comunicación y plataformas digitales y sus efectos en la Salud Mental 2026. Disponible en: https://www.concortv.gob.pe/wp-content/uploads/2026/09/CONSUMO-Y-ACCESO-DE-NNA-A-MEDIOS-DE-COMUNICACION-Y-PLATAFORMAS-DIGITALES-Y-SUS-EFECTOS-EN-LA-SALUD-MENTAL.pdf

[4] Fuente: https://www.gob.pe/institucion/insm/noticias/1443861-caso-meta-impacto-de-las-pantallas-en-la-salud-mental-de-ninos-y-adolescentes-y-retos-de-salud-publica-en-el-peru

[5] Fuente: https://www.aldeasinfantiles.org.pe/noticias/9-de-10-ninos-creen-riesgos-digitales-suicidio

mental de las niñas, niños y adolescentes (NNA). El estudio reveló que el 91% de NNA considera que amenazas como el ciberacoso, el grooming y la sextorsión pueden generar depresión e incluso llevar al suicidio. Por otra parte, según el mismo estudio, 3 de cada 10 adolescentes sienten ansiedad o desesperación cuando no pueden acceder a redes sociales o videojuegos. Además, el 54% ha sentido tristeza o molestia al ver casos de ciberacoso en su entorno escolar.

De otro lado, según un estudio de la Universidad Nacional del Centro[6], el 60% de los jóvenes peruanos evaluados presentó síntomas significativos de ansiedad y depresión directamente vinculados a la interacción digital. El 75% admitió utilizar redes sociales todos los días por un promedio de 4 horas. El análisis estadístico evidenció una correlación positiva directa: a mayor cantidad de horas en pantallas, mayores son los niveles de deterioro de la salud mental en menores vulnerables.

I.3. Mecanismos de atracción tecnológica y exposición a delitos informáticos

El problema se agrava por el diseño de los propios servicios digitales, los cuales incorporan patrones oscuros e interfaces adictivas orientadas a motivar el consumo y generar una demanda, lo que conlleva ingresos para quienes suministran las plataformas digitales:

a) **Mecanismos adictivos:** Existen mecanismos como la reproducción automática (*autoplay*), el desplazamiento infinito (*scroll* infinito), las rachas (*streaks*), las cajas de botín (*loot boxes*) y las apuestas en línea con publicidad segmentada en horarios familiares. La hiperconectividad es impulsada tanto por el diseño tecnológico persuasivo de las aplicaciones como por malas prácticas familiares donde los dispositivos asumen funciones de "niñera digital". Estos entornos digitales funcionan como espacios de socialización y construcción de identidad vinculada a la aceptación social como mecanismo de validación de la personalidad. Los niños y adolescentes asumen un rol activo de creadores de contenido, buscando ansiosamente su validación ("likes" y reacciones). En este aspecto, cabe destacar que las plataformas preferidas por este segmento poblacional son *TikTok, YouTube* e *Instagram*, seguidas por *WhatsApp* y videojuegos en línea como *Roblox* y *Minecraft*, con un tiempo de conexión diario promedio entre las dos y cuatro horas.[7]

b) **Exposición de menores a ser víctimas de delitos informáticos:** De acuerdo con encuestas del Instituto de Estudios Peruanos (IEP), aproximadamente 280 mil menores recibieron propuestas sexuales en línea y a 501 mil les solicitaron fotos de contenido explícito (mayormente adolescentes de 13 a 16 años)[8].

[6] Universidad Nacional del Centro. El impacto de las redes sociales en la salud mental de jóvenes en situación de vulnerabilidad en Huancayo. Disponible en: https://revistas.uncp.edu.pe/index.php/SD/article/view/2354

[7] Consejo Consultivo de Radio y Televisión – CONCORTV. Estudio sobre el Consumo y acceso de Niños, Niñas y Adolescentes a medios de comunicación y plataformas digitales y sus efectos en la Salud Mental 2026. Disponible en: https://www.concortv.gob.pe/wp-content/uploads/2026/09/CONSUMO-Y-ACCESO-DE-NNA-A-MEDIOS-DE-COMUNICACION-Y-PLATAFORMAS-DIGITALES-Y-SUS-EFECTOS-EN-LA-SALUD-MENTAL.pdf

[8] Perú21. Aumenta la explotación sexual on line a menores. Disponible en: https://peru21.pe/lima/aumenta-la-explotacion-sexual-online-menores-20230518203022/

Según un informe reciente de la UNICEF[9], "aproximadamente 20 millones de niños y adolescentes de entre 12 y 17 años —casi 1 de cada 5— fueron víctimas de alguna forma de explotación y abuso sexual facilitados por la tecnología en el transcurso de un año en 21 países".

Recientemente, el Ministerio de la Mujer y Poblaciones Vulnerables, durante la presentación de una encuesta relacionada con la "Percepción de niñas, niños y adolescentes frente a los riesgos de la explotación sexual en el entorno virtual", informó que el 49.4% de menores entrevistados manifestó haber conversado con personas desconocidas por internet y el 45.2% reportó haber vivido al menos una situación de riesgo en entornos digitales.

c) **Variedad y sofisticación de los riesgos producidos por entornos digitales**: En la actualidad, los niños y adolescentes se enfrentan de manera regular a riesgos complejos de violencia y explotación digital como el ciberacoso (cyberbullying), el grooming (captación mediante perfiles falsos en videojuegos abiertos como Roblox o Minecraft), la sextorsión y la exposición no consentida a contenidos nocivos (violencia, apuestas en línea/gambling, algoritmos de radicalización). Cabe precisar que dichos "riesgos" se encuentran vinculados con conductas tipificadas en nuestro Código Penal, como el ciberacoso (Art. 151-A), el *grooming* o captación sexual (Art. 183-B), la sextorsión (Art. 200), el *sexting* no consentido, la suplantación de identidad y el uso malicioso de *deepfakes* mediante Inteligencia Artificial.

II. EVIDENCIA QUE SUSTENTA EL PROBLEMA

Las plataformas digitales no garantizan adecuados elementos de seguridad para niños y adolescentes, y la ausencia de regulación apropiada permite que herramientas como las VPN (Virtual Private Network o Redes Privadas Virtuales) sean mal utilizadas para eludir restricciones, dificultando la supervisión y protección.

Se ha verificado que un uso intensivo e incontrolado de pantallas, redes sociales y videojuegos genera un círculo vicioso de afectación socioemocional acreditado por la evidencia sanitaria del Ministerio de Salud (MINSA) y del Instituto Nacional de Salud Mental (INSM):

a) **Graves problemas de salud mental y disposición al suicidio**: Según información proporcionada por la directora general del Hospital Nacional Víctor Larco Herrera[10], Judy López Arias, más de tres millones de adolescentes presentan problemas de salud mental en nuestro país. Asimismo, manifestó que 36 de cada 100 adolescentes presentaron conducta suicida en el año 2024.

b) **Trastornos en la conducta y déficit de atención:** Según información proporcionada por el Ministerio de Salud[11] se conoce que 1 de cada 10 niños de 6 a 11 años padece de Trastorno de déficit de atención e hiperactividad TDAH,

[9] Fuente: *Through Children's Eyes: How Digital Technologies Enable Child Sexual Abuse*. Disponible en: https://www.unicef.org/press-releases/1-5-children-across-21-countries-have-experienced-tech-facilitated-sexual

[10] Fuente: https://comunicaciones.congreso.gob.pe/noticias/comision-ocde-recibio-informacion-sobre-el-estado-de-salud-mental-en-el-pais/

[11] Ministerio de Salud (MINSA), Implementación de las leyes 31405 y 31887, Comisión Multisectorial de Alto Nivel en Materia de Protección de Niñas, Niños y Adolescentes en Situación de Orfandad, presentación ante la Comisión de Salud del Congreso de la República, realizada el 05.09.2025

aproximadamente 314,000 casos. Asimismo, el sistema de salud atendió a 1,324 adolescentes por casos de juego patológico.

A nivel mundial, según la Organización Mundial de la Salud (OMS) y la American Psychiatric Association (APA)[12] la ciberadicción y la adicción a juegos en línea ostentan una prevalencia que fluctúa entre el 3% y el 10% (CIE-11 y DSM-5).

c) **Afectación neurobiológica y del sueño:** La exposición nocturna a pantallas inhibe la secreción de melatonina debido a la luz azul, provocando alteraciones severas del sueño que deterioran el rendimiento académico y el estado de ánimo. La sobreestimulación por más de tres horas diarias en redes sociales impacta áreas cerebrales como la amígdala, incrementando síntomas ansioso-depresivos y conductas evasivas o compulsivas[13]. El uso excesivo de dispositivos móviles y entornos digitales, de forma descontrolada, está generando síntomas como ansiedad, irritabilidad, trastornos del sueño, bajo rendimiento escolar e incluso aislamiento social en niños cada vez de menor edad.

La evidencia expuesta precedentemente nos lleva a considerar la necesidad impostergable de regular el uso de los entornos digitales, por parte Por otra parte, resulta importante destacar que, según datos de una encuesta realizada por IPSOS[14], el año 2024, conscientes del riesgo que conlleva el entorno digital, el 38% de los peruanos cree que el uso de la IA (incluido ChatGPT) debería estar prohibido en las escuelas. Además, 74% de peruanos conectados cree que se debe prohibir a los niños menores de 14 años el uso de redes sociales tanto dentro como fuera de la escuela.

III. OBJETIVOS GENERALES Y ESPECÍFICOS

Objetivo general:

Establecer el marco jurídico y digital para regular el acceso, permanencia y uso de plataformas de redes sociales por parte de menores de 16 años en el territorio nacional. La finalidad es salvaguardar su integridad psicofísica, proteger sus datos personales y promover el desarrollo de una ciudadanía digital responsable. Además, se debe equilibrar salvaguardar su integridad psicofísica, proteger sus datos personales y promover el desarrollo de una ciudadanía digital responsable, equilibrando la innovación tecnológica con el interés superior del niño y del adolescente.

Objetivos específicos:

a) Establecer normas de seguridad y privacidad por defecto para las plataformas, aplicaciones, redes sociales y videojuegos disponibles en el mercado peruano, exigiendo la inhabilitación predeterminada de funciones adictivas (como la reproducción automática, el desplazamiento infinito y las rachas) para usuarios menores de edad.

---

[12] la Organización Mundial de la Salud (OMS) mediante la Clasificación Internacional de Enfermedades (CIE-11, que incorporó el *Gaming Disorder*) y la American Psychiatric Association (APA) mediante el DSM-5 (*Internet Gaming Disorder*).

[13] Fuente: https://www.gob.pe/institucion/minsa/noticias/30804-el-uso-excesivo-de-los-dispositivos-electronicos-por-ninos-es-de-alto-riesgo-para-su-salud-mental

[14] IPSOS. Monitor Global de la Educación 2024. Disponible en: https://www.ipsos.com/es-pe/monitor-global-de-educacion-2024

b) Garantizar que las empresas operadoras de servicios públicos de telecomunicaciones brinden información clara y pongan a disposición de los usuarios mecanismos de control parental y filtros de contenido, administrando el marcador de estado pseudoanonimizado (RDU-NA) sin inspeccionar el tráfico de comunicaciones ni vulnerar el principio de neutralidad de red.

c) Promover la participación parental orientativa en los hogares para la supervisión y mediación del uso de la tecnología, facilitando el acceso a recursos públicos de apoyo (como el catálogo y guía de herramientas "Modo Aprendizaje" de la PCM)

d) Distribuir las competencias de supervisión y política pública según la especialidad de cada entidad: la PCM en la articulación multisectorial; el MINEDU en la inclusión de la ciudadanía digital y protocolos pedagógicos en escuelas; el MINSA en la prevención sanitaria y guías de salud mental; y la ANPD, INDECOPI u OSIPTEL en la fiscalización de sus respectivas materias.

IV. FUNDAMENTACIÓN DE LA INICIATIVA

El problema público en el Perú, respecto a los entornos digitales, radica en la **exposición desprotegida de los menores a los medios digitales adictivos y no supervisados**, sumada a un vacío regulatorio que no exige responsabilidad por diseño a los proveedores tecnológicos. Es decir, el problema no es el acceso a la tecnología, sino la amplitud y diversidad de contenido que se encuentra disponible para el consumo de menores, no a menudo apto para el nivel de desarrollo psicofísico de los niños y adolescentes.

Las empresas operadoras de telecomunicaciones solo proveen conectividad y no pueden inspeccionar ni filtrar tráfico, siendo una herramienta opcional ofrecida al abonado y no de filtrado en red. Por tanto, los estándares de diseño seguro (privacidad por defecto, desactivación de funciones adictivas, restricciones de mensajería con desconocidos y paneles de gestión del tiempo) deben recaer directamente en la capa de proveedores de servicios y plataformas digitales. Esto debe hacerse bajo la supervisión de la Autoridad Nacional de Protección de Datos Personales (ANPD) e INDECOPI en materia publicitaria.

El marco legal peruano vigente presenta severas limitaciones para hacer frente a esta problemática. Toda vez que la Ley 30254 (Ley de Promoción para el Uso Seguro y Responsable de las TIC) posee un enfoque declarativo y de sensibilización general, pero carece de herramientas concretas para exigir responsabilidades técnicas a los proveedores de dispositivos móviles y de plataformas digitales.

De otro lado, la Ley 29733 (Ley de Protección de Datos Personales) regula el consentimiento de datos, pero no contemplaba salvaguardas específicas respecto a la administración de datos personales, ni la publicidad personalizada dirigida a menores.

En razón de ello, la solución legal integral requiere actualizar el marco vigente, mediante la reforma de la Ley 30254 y la adecuación de la Ley 29733, bajo un modelo de corresponsabilidad tripartita (familia, Estado y proveedores). En ese sentido, la presente iniciativa legislativa comprende un diseño integral y comprensivo de los varios aspectos del fenómeno y de los actores que tienen un rol y responsabilidad en la búsqueda de

una solución a este problema. Además, supera dos enfoques divergentes: las propuestas de prohibición absoluta o la autorregulación sin interferencias del Estado

Por ello, el núcleo de la propuesta comprende cuatro componentes relevantes:

a) **Gradualidad etaria:** Consentimiento digital autónomo a partir de los 16 años e intervención/autorización de los padres para menores de 16.

b) **Deberes de diligencia parental orientativa:** Sin régimen sancionador para las familias.

c) **Obligaciones de resultado para plataformas:** Privacidad por diseño, prohibición de publicidad personalizada basada en perfilado y entornos digitales seguros ajustados al desarrollo integral y bienestar de la niñez.

d) **El rol subsidiario del Estado**, que establece el rol de los actores públicos involucrados en el diseño del marco normativo, herramientas de orientación y fiscalización de las reglas de alcance general respecto al de uso de los dispositivos móviles para los niños y adolescentes

V. MARCO LEGAL NACIONAL Y LEGISLACIÓN INTERNACIONAL

V.1. Marco legal nacional

a) Ley 28278 Ley de Radio y Televisión Establece el horario familiar para medios tradicionales. Vigente, pero no alcanza a los medios digitales, sujetos solo a una autorregulación.

b) Ley 30254 y su modificatoria Ley 31664, Ley de Promoción para el Uso Seguro y Responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes

Constituye la norma marco inicial que fija los lineamientos para proteger a los menores de los riesgos de Internet, promoviendo acciones educativas de prevención y la obligación de las empresas operadoras de ofrecer filtros de contenido nocivo.

c) Ley 32385, Ley que regula el uso de teléfonos celulares en todas las instituciones y programas educativos de la educación básica y su Reglamento D.S. Nº 018-2026-MINEDU

Tiene por finalidad regulación del uso de dispositivos electrónicos en el entorno escolar, para reducir la sobreexposición al internet, combatir el ciberbullying, prevenir trastornos de salud mental y mejorar el rendimiento académico.

d) Ley 29733, Ley de Protección de Datos Personales y su Reglamento D.S. 016-2024-JUS

Establece las reglas para el tratamiento de datos personales de menores de edad, definiendo las condiciones para el consentimiento informado y la privacidad digital en línea.

V.2. Legislación internacional

El marco regulatorio internacional sobre la protección de niños y adolescentes en entornos digitales presenta una clara evolución: se ha pasado de modelos basados en

la autorregulación del usuario o el control rígido y coercitivo familiar o por parte estatal, a un enfoque de debida diligencia con responsabilidad en la capa de servicios (*safety and privacy by design*). Este modelo busca equilibrar la tutela del desarrollo integral y la salud mental con el respeto a los derechos de acceso a la información, educación y libertad de expresión, tal como lo establece la Observación General N.º 25 de la Convención sobre los Derechos del Niño de la ONU, que establece que los derechos de los niños, niñas y adolescentes deben ser respetados, protegidos y garantizados plenamente en el entorno digital.

1. **AUSTRALIA (Online Safety Amendment - Social Media Minimum Age Act 2024 No. 127)[15]**

Esta norma, Ley de Enmienda de Seguridad en Línea sobre la Edad Mínima en Redes Sociales de 2024, n.º 127 de 2024, ha entrado en vigor el 10 de diciembre del 2025. Entre otras medidas, establece una edad mínima de 16 años para la creación y gestión autónoma de cuentas en plataformas digitales clasificadas como "redes sociales restringidas por edad". La norma obliga a las plataformas a implementar salvaguardas efectivas en favor de los menores (como auditorías de verificación o estimación de edad mediante IA o datos biométricos), proporcionales y no intrusivas, prohibiendo expresamente la exigencia indiscriminada de documentos oficiales para proteger la privacidad de los menores. Excluye explícitamente plataformas de mensajería, videojuegos y herramientas educativas, tales como, *WhatsApp, Google Classroom, Discord, Roblox y YouTube Kids.* Asimismo, este instrumento normativo pionero fija sanciones significativas para las corporaciones tecnológicas ante el incumplimiento de las disposiciones de la ley.

2. **REINO UNIDO (Age Appropriate Design Code - AADC / ICO)[16]**

Este instrumento normativo, también conocido como el Children's Code, fue redactado por la Oficina del Comisionado de Información del Reino Unido (ICO) bajo el mandato de la Ley de Protección de Datos de 2018 (*Data Protection Act 2018). Su* cumplimiento es obligatorio y auditable desde el 2 de septiembre de 2021.

Establece 15 estándares técnicos aplicables a servicios digitales dirigidos a menores de 18 años. Las empresas deben realizar obligatoriamente una Evaluación de Impacto de la Protección de Datos (DPIA) antes de lanzar cualquier servicio. Si no pueden determinar con certeza la edad de sus usuarios, el estándar dicta que deben aplicar las protecciones del código a **toda su base de usuarios**. Exige la configuración predeterminada de alta privacidad, transparencia en los términos de servicio, verificación de edad y la desactivación obligatoria de funciones de diseño adictivo (como el desplazamiento infinito, la reproducción automática o las notificaciones excesivas). Su incumplimiento conlleva la aplicación de las mismas multas civiles masivas de la protección de datos europea: hasta **17.5 millones de libras esterlinas (GBP)** o el **4% de la facturación global anual** de la empresa tecnológica (lo que sea mayor).

También cabe mencionar otros instrumentos normativos: en 2025 y 2026, con posterioridad a la aprobación de la ley marco, el regulador británico de las comunicaciones (Ofcom) redactó y sometió a consulta parlamentaria códigos

[15] Fuente: https://www.legislation.gov.au/C2024A00127/asmade/text

[16] Fuente: https://evalian.co.uk/childrens-code/

específicos. Los códigos de protección a la infancia (*Protection of Children Codes*) se emitieron formalmente en **julio de 2025**, mientras que los códigos de enmiendas frente a contenido ilegal (*Illegal Content Codes of Practice*) se terminaron de actualizar formalmente entre **mayo, junio y septiembre de 2026.**

3. UNIÓN EUROPEA (UE)[17]

a) **La Ley de Servicios Digitales** (conocida globalmente por sus siglas en inglés, **DSA** *Digital Services Act*, Reglamento UE 2022/2065), está vigente desde el 16 de noviembre del año 2022). Las plataformas tienen prohibido presentar anuncios basados en el perfilamiento de datos personales

La ley establece que las plataformas digitales tienen la obligación de realizar evaluaciones de riesgo y garantizar la transparencia de sus algoritmos frente a usuarios que son menores de edad.

Las grandes corporaciones deben evaluar anualmente e implementar planes de mitigación obligatorios respecto a los efectos negativos que sus servicios provocan en los menores. La ley tipifica de manera explícita la obligación de analizar y frenar:

- El impacto en la salud física y mental de los menores (diseños adictivos, "infinitos" o que promueven la depresión y trastornos alimenticios).
- El acceso a contenidos nocivos (violencia, incitación al odio o desinformación).
- El menoscabo de los derechos fundamentales del niño

La Comisión Europea supervisa directamente a las plataformas digitales más grandes y tiene la facultad legal de imponer multas de hasta el 6% de la facturación global anual de la empresa en caso de incumplimiento de sus responsabilidades.

b) Directiva de Servicios de Medios Audiovisuales (AVMSD)[18]

La AVMSD, Directiva del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, Directiva 2018/1808, introduce una serie de obligaciones con relación a la protección de menores

Impone restricciones estrictas a la publicidad perjudicial dirigida a menores y establece salvaguardas contra la exposición a contenidos violentos o pornográficos.

Regulación Obligatoria de las Plataformas de Intercambio de Videos

NUEVA Propuesta de la EU KIDS Act (17 de septiembre de 2026):

Establece la modalidad de acceso gradual por edades (Graduated Approach). **Prohíbe el acceso a cuentas de redes sociales a menores de 13 años** (solo permite video en línea, adecuado bajo perfil gestionado por tutores). De 13 a 14 años, habilita "mini-cuentas" bajo control parental con un límite máximo de pantalla de 1 hora diaria y funciones restringidas. A partir de los 15 años se permite la creación autónoma de cuentas. Se exige, asimismo, el uso de mecanismos como la aplicación de verificación de edad de la UE, que no almacena documentos de identidad ni datos biométricos.

[17] Fuente: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065

[18] Fuente: https://www.boe.es/doue/2018/303/L00069-00092.pdf

Se invierte la carga de la prueba (*Safe by Design*), ello implica que corresponde a las plataformas demostrar técnicamente que sus servicios son seguros para menores. Se prohíben por defecto el scroll infinito, las notificaciones emergentes durante horas de descanso y los chatbots/compañeros de IA que conllevan dependencia emocional.

Con esta nueva propuesta se pasaría de la prohibición rígida al Acceso Gradual Etario: La EU KIDS Act consolida la tendencia de no vetar totalmente la tecnología, sino modular las funciones según el nivel de desarrollo (13, 15 y 16 años).

Asimismo, se propone la desactivación obligatoria de agentes de IA Emocionales. Por primera vez se regula explícitamente el impacto de asistentes de IA y chatbots conversacionales en la salud mental infantil.

4. ESTADOS UNIDOS

En la actualidad, 2026, la regulación en los Estados Unidos de Norteamérica para proteger a los menores en entornos digitales se divide en un **marco federal vigente, pero bajo reforma**, y una variedad **de leyes estatales restrictivas** que intentan amortiguar el impacto de las redes sociales en la vida de los niños y adolescentes.

A nivel federal, la única ley sobre la materia, plenamente vigente y aplicable en 2026, es la **Children's Online Privacy Protection Act (COPPA)**[19], vigente desde 1998

Esta ley tiene entre sus características más relevantes:

a) **Consentimiento Paterno:** Establece la obligación para los sitios web y aplicaciones comerciales de obtener consentimiento verificable de los padres antes de recopilar, utilizar o divulgar información personal de niños menores de 13 años. Limita la publicidad dirigida

b) **Ampliación de "Datos Personales":** A partir de algunas reformas que entraron en vigor en 2026 expandieron la definición de datos protegidos para incluir explícitamente identificadores biométricos y datos de geolocalización precisos.

c) **Responsabilidad de Terceros:** Las plataformas son responsables si sus redes de publicidad o complementos (*plug-ins*) recopilan datos de menores, bajo conocimiento de estas. Estas trasgresiones se sancionan con multas que superan los $53,000 por infracción

A nivel de leyes estatales específicas, otro instrumento normativo específico relevante es la Children's Internet Protection Act (CIPA), la que obliga a las escuelas y bibliotecas públicas receptoras de fondos federales a implementar filtros tecnológicos para bloquear material obsceno, pornografía infantil o nocivas para menores de edad.

5. ESPAÑA

Durante el **2025**, España ha impulsado su mayor transformación legal en materia de protección de menores ante entornos digitales. El marco normativo se encuentra en revisión, encontrándose en trámite en las Cortes Generales de España (Cámara de Diputados), el Proyecto de Ley Orgánica para la protección de las personas menores de

[19] Fuente: https://usercentrics.com/knowledge-hub/childrens-online-privacy-protection-act-coppa/

edad en los entornos digitales[20] el cual es un ambicioso paquete impulsado por el Gobierno con el objetivo explícito de prohibir el acceso de menores de 16 años a las redes sociales, el que aún no ha logrado convertirse en ley. Entre las principales características de este instrumento normativo se pueden mencionar las siguientes:

a) Prohibición y Elevación de Edad: Se eleva de 14 a 16 años la edad mínima para consentir el tratamiento de datos personales para abrir perfiles en plataformas digitales y redes sociales. Por debajo de esa edad, el acceso queda estrictamente prohibido, eliminando incluso la posibilidad de saltarse el bloqueo mediante autorización parental.

b) Verificación de Edad Obligatoria: Obliga a las tecnológicas a implementar una herramienta pública, segura y gratuita de verificación de edad (basada en el estándar de la app desarrollada junto a la Agencia Española de Protección de Datos) para impedir que los menores evadan las restricciones.

c) Control Parental de Fábrica: Todos los teléfonos móviles, tabletas y ordenadores nuevos vendidos en España deben incorporar un sistema de control parental gratuito activable desde el primer encendido, además de un etiquetado claro que alerte de los riesgos del dispositivo.

d) Multas Millonarias: Las empresas tecnológicas que incumplan las medidas de protección se exponen a sanciones económicas severas gestionadas por la Comisión Nacional de los Mercados y la Competencia (CNMC), que pueden alcanzar los 2 millones de euros.

6. BRASIL

La protección de los menores ante los entornos digitales en Brasil está regida por una de las legislaciones consideradas entre las más estrictas e integrales a nivel mundial, la Ley Nº 15.211/2025, conocida oficialmente como el **ECA Digital** (*Estatuto Digital de la Niñez y la Adolescencia*).

"En cuanto a las obligaciones impuestas, la norma establece un conjunto robusto de deberes para los proveedores de servicios digitales, entre los que se destacan: (i) la implementación de mecanismos fiables de verificación de edad, destinados a restringir el acceso a contenidos inapropiados para menores de 18 años; (ii) la prohibición de permitir la creación de cuentas por parte de menores en plataformas que ofrezcan contenido pornográfico; (iii) la obligación de brindar información clara y accesible a padres, tutores, niños y adolescentes sobre riesgos digitales, medidas de seguridad, entre otras; (iv) la prohibición de mecanismos de monetización como las *loot boxes* en videojuegos dirigidos a menores o accesibles según su clasificación etaria; (v) la restricción del uso de técnicas de perfilado para dirigir publicidad a niños y adolescentes; (vi) la obligación de vincular cuentas de usuarios menores de 16 años con las de sus padres o tutores legales; y (vii) el deber de eliminar y reportar a las autoridades

[20] Fuente: https://www.mpr.gob.es/servicios/participacion/audienciapublica/Documents/VSGT%202024/2024-0921%20APLO%20menores%20entornos%20digitales/MAIN.pdf

competentes cualquier contenido que evidencie explotación o abuso sexual infantil, secuestro o incitación."[21]. En caso de incumplimiento, la legislación establece multas

drásticas de hasta el 10% de la facturación de la empresa en Brasil o un tope de 50 millones de reales, incluyendo la potestad de decretar la suspensión inmediata de las operaciones de la plataforma en el país.

7. COLOMBIA

En Colombia, la protección de menores ante entornos digitales está regulada por Ley reciente[22], la Ley 2489 de 2025, reglamentada por el Decreto 0769 de 2026. El Decreto de 2026 impone cargas éticas y algorítmicas directas a las plataformas digitales. Prohíbe de manera categórica el perfilamiento algorítmico comercial, la recopilación de datos biométricos y el rastreo de ubicación de menores con fines publicitarios. Además, exige la verificación efectiva de la edad y la revisión de sistemas de recomendación para evitar conductas adictivas. Las plataformas digitales (*Meta, TikTok, YouTube*, etc.) tienen la obligación técnica de implementar sistemas eficaces de verificación de edad y canales de reporte inmediato conectados las veinticuatro horas del día. Las entidades públicas encargadas del control son el Ministerio TIC y Superintendencia de Industria y Comercio.

8. PARAGUAY

En el Paraguay, la normatividad legal dirigida a proteger a los menores en entornos digitales tiene su expresión actual en la Ley 5653/2016 y en el Decreto 8098/2022[23]. En dichos instrumentos normativos, se establece la obligación de los proveedores de servicios de internet (ISP) a suministrar software gratuito de filtrado y bloqueo de contenidos nocivos, junto con herramientas de control parental. El mecanismo opera a nivel de infraestructura de telecomunicaciones (como bloqueo por DNS seguro). El control se efectiviza a través de la fiscalización de la infraestructura de los ISP y locales públicos. El organismo público encargado del control estatal es el CONATEL (Comisión Nacional de Telecomunicaciones)

9. OCDE

En su reciente estudio, publicado en marzo del 2026, titulado "Crecer en la era de las redes sociales"[24], la OCDE, destaca que la infancia está plenamente inmersa en la era digital (el 93% de los niños ya está conectado a los 10 años), pero esto ha detonado una crisis de bienestar y una ola regulatoria global impulsada por el preocupante aumento del uso problemático

En otro estudio, del año 2025, titulado ¿Como es la vida de los niños en la era digital?[25] Se señala que las plataformas de IA pueden exacerbar los riesgos que se experimentan

[21] Fuente: https://allende.com/privacidad-y-ciberseguridad/eca-digital-brasil-regula-la-proteccion-de-menores-en-entornos-digitales-04-17-2026/

[22] Fuente: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/439846:Colombia-fortalece-la-proteccion-de-ninas-ninos-y-adolescentes-con-el-Decreto-de-Entornos-Digitales-Sanos-y-Seguros

[23] Fuente: https://siteal.iiep.unesco.org/bdnp/405/ley-56532016-ley-proteccion-ninos-ninas-adolescentes-contra-contenidos-nocivos-internet

[24] Fuente: https://www.oecd.org/en/publications/growing-up-in-the-social-media-age_a1132839-en.html

[25] Fuente: https://www.oecd.org/en/topics/children-in-the-digital-environment.html

en línea, entre ellos: Exposición a la desinformación y la información errónea, Preocupaciones sobre privacidad y seguridad, Impacto mental y emocional.

La realidad virtual también puede amplificar experiencias negativas, como el ciberacoso y el hostigamiento, el aislamiento y los problemas de salud mental, mientras que el contenido de ritmo rápido puede agotar las funciones cognitivas y dificultar el desarrollo de las habilidades ejecutivas. La naturaleza inmersiva de la RV se cruza con el desarrollo cognitivo de los niños, afectando su capacidad para distinguir las experiencias virtuales de la realidad.

La principal directriz de la OCDE es exigir que las empresas tecnológicas apliquen el principio de "Seguridad Digital por Diseño" (*Digital Safety by Design*). Los filtros y salvaguardas deben aplicarse en la capa de servicios y aplicaciones (software y redes sociales) y no en la infraestructura de transporte o telecomunicaciones, garantizando el respeto al principio de neutralidad de red. Esto obliga a las plataformas a integrar sistemas de verificación de edad fiables, configuraciones de privacidad estrictas por defecto y entornos centrados en el interés superior del menor, en lugar de depender únicamente de la vigilancia parental.

Asimismo, se expresa poca confianza en las medidas prohibitivas rígidas (como bloqueos universales de internet, registros estatales de dispositivos por IMEI o bloqueos de VPN), las que han demostrado ser ineficaces, ya que los menores eluden las restricciones mediante identidades falsas o redes privadas, desplazándose a entornos digitales aún más inseguros. Por ello, el consenso promueve la gradualidad etaria, las herramientas de control parental opcionales y la alfabetización digital.

10. UNICEF

La UNICEF[26] exige que las empresas tecnológicas no pueden sustraerse a su obligación de diseñar y organizar sus plataformas digitales, configurándolas bajo un enfoque de derechos de la infancia. No se debe delegar toda la responsabilidad de la protección en los padres.

Entre las principales propuestas de la UNICEF, podemos encontrar:

a) Plataformas con "Seguridad desde el Diseño" (Safety by Design): las cuentas de menores deben ser privadas de forma automática desde el momento de su creación.
b) Fortalecimiento de Sistemas de Apoyo Integrales: en el marco de la protección infantil en el entorno digital, los gobiernos deben invertir en infraestructura de respuesta.
c) Corresponsabilidad Ética y Regulación de la Inteligencia Artificial: los Estados deben actualizar sus códigos penales para sancionar el uso de Inteligencia Artificial en la creación de material de abuso sexual infantil o la generación de *deepfakes* pornográficos.
d) Alfabetización y Acompañamiento sin Invasión: superar el control autoritario por una "crianza digital positiva" y acompañar a los menores sin invadir su privacidad.

[26] Fuente: Zoom a las infancias y adolescencias en la era digital. Disponible en: https://www.unicef.org/argentina/media/28056/file/Zoom%20a%20las%20infancias%20y%20adolescencias%20en%20la%20era%20digital.pdf

e) Participación de los Menores en la Solución: propone crear vías seguras y participativas para que los adolescentes aporten en el debate y en la construcción de los entornos digitales que ellos mismos

VI. ANTECEDENTES LEGISLATIVOS, INVESTIGACIONES Y FUENTES UTILIZADAS

a) Proyecto de Ley 8017/2023-CR, presentado por la congresista Yessica Rosselli Amuruz Dulanto, el 31 de mayo de 2024, mediante el cual **"**Propone promover la salud integral de los niños y adolescentes en el desarrollo de su etapa escolar, en las instituciones educativas públicas y privadas de la educación básica regular, para la prevención e identificación temprana de enfermedades". La Comisión de Salud y Población aprobó por mayoría, el 9 de febrero de 2026, un texto sustitutorio denominado "Ley de promoción y prevención en salud mental para niños, niñas y adolescentes en entornos digitales seguros"

b) Proyecto de Ley 10880/2024-CR, presentado por el congresista George Edward Málaga Trillo, el 21 de abril de 2025, "Ley de protección de niños y adolescentes en entornos digitales", mediante el cual **p**ropone "establecer un marco regulatorio integral para prevenir y mitigar los efectos nocivos que pantallas, dispositivos móviles y redes sociales pueden tener en la salud mental de niños y adolescentes. para ello, promueve entornos digitales seguros y con énfasis educativo, fijando límites razonables de uso para menores, herramientas y recomendaciones para padres y tutores, y obligaciones para los proveedores de dichos servicios". Fue decretado a la Comisión de Mujer y Familia (primera comisión dictaminadora) y a la Comisión de Salud y Población (segunda comisión dictaminadora). La Comisión de Mujer y Familia aprobó por mayoría, el 3 de noviembre de 2025, un texto sustitutorio denominado "Ley de protección y bienestar digital de niños y adolescentes en entornos digitales y servicios en línea". La Comisión de Salud y Población aprobó por mayoría, el 9 de febrero de 2026, un texto sustitutorio denominado "Ley de promoción y prevención en salud mental para niños, niñas y adolescentes en entornos digitales seguros"**.**

Cabe señalar que la presente propuesta legislativa se fundamenta en este proyecto de ley (10880). No obstante, cabe precisar que para la elaboración de la fórmula legal de la presente propuesta legislativa se ha tomado, también, el texto sustitutorio de la fórmula legal contenido en el dictamen aprobado por la Comisión de Mujer y Familia, al que se le han incorporado algunas modificaciones que se han considerado pertinentes, acordes con la evolución de la problemática, acaecida en tiempos recientes.

c) Proyecto de Ley 13453/2025-CR, presentado por la congresista Magaly Ruíz Rodríguez, el 03 de diciembre de 2025, mediante el cual "Propone establecer un marco para la promoción, prevención y fortalecimiento de capacidades dirigidas a proteger y mejorar la salud mental de niños y adolescentes en su interacción en entornos digitales, así como a potenciar sus beneficios educativos, sociales y recreativos". Fue decretado a la Comisión de Mujer y Familia (primera comisión dictaminadora) y a la Comisión de Salud y Población. La Comisión de Salud y Población aprobó por mayoría, el 9 de febrero de 2026, un texto sustitutorio denominado "Ley de promoción y prevención en salud mental para niños, niñas y adolescentes en entornos digitales seguros".

VII. SECTORES COMPRENDIDOS

a) **Presidencia del Consejo de ministros (PCM):** Promueve la creación y preside la **Comisión Multisectorial permanente** encargada de articular, coordinar y

monitorear las políticas públicas de salud mental y bienestar digital de menores. Asimismo, remite el informe consolidado anual al Congreso de la República.

- **Secretaría de Gobierno y Transformación Digital (PCM):** Ejerce la Secretaría Técnica de la Comisión Multisectorial y tiene a su cargo la implementación y difusión del módulo **«Modo Aprendizaje»** como un ecosistema digital de herramientas, guías y recursos gratuitos de apoyo a padres, madres o tutores para la configuración de perfiles para niños adolescentes, controles parentales y opciones de privacidad por defecto.

b) Ministerio de Educación (MINEDU): Promueve la inclusión de contenidos de ciudadanía y seguridad digital en el Currículo Nacional, capacita a los docentes para prevenir e identificar la violencia digital y fija las reglas sobre el uso de dispositivos móviles en las instituciones educativos.

c) Ministerio de Salud (MINSA): Elabora guías técnicas sanitarias sobre el uso problemático de pantallas, aprueba los mensajes de advertencia sanitaria obligatorios, fortalece los servicios de orientación/teleorientación y emite un reporte anual sobre salud mental digital.

d) Ministerio de la Mujer y Poblaciones Vulnerables (MIMP): Lidera las acciones de prevención, atención y derivación oportuna ante situaciones de violencia digital (ciberacoso, grooming, sextorsión) y promueve programas de orientación para el acompañamiento familiar.

e) Ministerio de Transportes y Comunicaciones (MTC): Es el ente rector y regulador en el sector telecomunicaciones, participa en la clasificación técnica de dispositivos y canaliza la recaudación del canon del espectro radioeléctrico (del cual el 10% se destina a investigación en salud mental).

f) Ministerio del Interior (MININTER): Integra la Comisión Multisectorial para la articulación en prevención de ciberdelitos e inseguridad digital que afecte a menores.

g) La Autoridad Nacional de Protección de Datos Personales (ANPD): Es responsable del diseño, administración, supervisión y control del Registro de dispositivos móviles de uso por niños y adolescentes

h) El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI): Es responsable de fiscalizar que las empresas operadoras que comercialicen dispositivos incluyan los mensajes y etiquetas preventivas aprobados por el MINSA sobre los riesgos para la salud mental y el bienestar de los niños y adolescentes en su interacción con el entorno digital.

i) El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL): Supervisa, fiscaliza y sanciona a las empresas operadoras de telecomunicaciones respecto al cumplimiento de sus obligaciones (activación del marcador de estado, disponibilidad de controles parentales y canales de atención).

j) El Consejo Nacional de Ciencia, Tecnología e Innovación (CONCYTEC): En coordinación con el MINSA, promueve la investigación científica sobre el impacto de las tecnologías, redes sociales y videojuegos en el desarrollo cognitivo y la salud mental infantil, administrando los fondos provenientes del canon.

k) Municipalidades provinciales y distritales: Sancionan a los establecimientos con acceso público a internet (como cabinas, restaurantes o plazas públicas) que no apliquen filtros contra contenido pornográfico o no respeten las reglas de acceso.

l) Defensoría del Pueblo: Participa en la Comisión Multisectorial como invitada permanente con voz, pero sin voto.

VIII. NORMAS QUE SE MODIFICAN O DEROGAN

CUADRO DE NORMAS QUE SE MODIFICAN O DEROGAN

Norma Afectada	Artículo / Disposición	Tipo de Modificación	Texto Propuesto
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 2** (inc. 20)	**Incorporación**	Agrega la definición de **"Protección de datos del niño y del adolescente"**, definiéndola como el conjunto de principios, derechos y garantías aplicables al tratamiento de sus datos en entornos digitales, priorizando el interés superior del niño y la privacidad.
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 5** (2. ° párrafo)	**Incorporación**	Exige que el consentimiento para el tratamiento de datos de NNA en entornos digitales garantice autorizaciones correspondientes y **mecanismos efectivos de verificación, control parental y seguridad** según el reglamento.
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 13** (numeral 13.3)	**Modificación / Sustitución**	Dispone medidas especiales por reglamento para el tratamiento de datos de NNA. Establece que los adolescentes

			de **16 a menos de 18 años** pueden otorgar **consentimiento informado autónomo**, siempre que la información sea clara.
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 16** (4. ° párrafo)	**Incorporación**	Obliga al titular del banco de datos o responsable en plataformas digitales a realizar **esfuerzos razonables para verificar la edad** de quienes otorgan su consentimiento, según la tecnología disponible.
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 20** (5. ° párrafo)	**Incorporación**	Incluye expresamente el **"derecho al olvido digital"** para NNA, permitiendo la eliminación de datos o contenidos publicados sin autorización cuando representen un riesgo para su integridad, seguridad o privacidad.
Ley 29733 (Ley de Protección de Datos Personales)	**Art. 33** (núm. 6)	**Modificación**	Amplía las funciones de la **Autoridad Nacional de Protección de Datos Personales (ANPD)** para coordinar con **MINEDU** y **MIMP** estrategias formativas, campañas de sensibilización y asistencia ante vulneraciones digitales.
Decreto Legislativo 702 (Promoción de la Inversión Privada en Telecomunicaciones)	**Art. 63**	Modificación	Dispone que el **10 % de lo recaudado por concepto de canon** por el uso del espectro radioeléctrico se destine a **financiar proyectos de investigación**

			relacionados con trastornos asociados a la adicción a dispositivos móviles y servicios digitales en niños y adolescentes."
Ley 30254 (Uso Seguro y Responsable de TIC por NNA)	**Toda la norma**	**Derogación Expresa Única**	Deroga de forma íntegra la Ley 30254.

IX. ANALISIS COSTO BENEFICIO

A. Costos para el Sector Público

La entrada en vigor de la presente ley no implica incremento en el gasto público o demanda de recursos adicionales al Tesoro Público. No contiene iniciativa de gasto, no contraviene el artículo 79 de la Constitución Política. Las acciones a cargo de los ministerios y organismos públicos (PCM, MINEDU, MINSA, MIMP) se ejecutan con cargo al presupuesto institucional de cada pliego.

Se reorientan recursos estatales ya percibidos sin impactar las finanzas de las empresas ni la tarifa de los usuarios. Tal como lo dispone el artículo 21 de la propuesta legislativa, se dispone una asignación presupuestal interna del 10% de lo recaudado por concepto de canon del espectro radioeléctrico (modificando el Decreto Legislativo 702), dirigido al Fondo de Salud Mental para financiar la investigación sobre adicciones digitales administrada por CONCYTEC.

De otro lado, la implementación de la presente iniciativa, propone aprovechar la capacidad instalada y la especialidad de las autoridades regulatorias existentes (ANPD para datos personales, INDECOPI para consumo y publicidad, OSIPTEL/MTC para telecomunicaciones) sin disponer la creación de nuevas entidades reguladoras ni burocracia paralela que aumente el gasto público.

B. Costos de Cumplimiento para el Sector Privado

Las obligaciones recaen sobre los proveedores de servicios digitales (redes sociales, apps, videojuegos) para que adapten sus interfaces mediante configuraciones por defecto protectoras (privacidad reforzada, restricciones de mensajería con desconocidos, avisos de descanso y paneles de gestión de tiempo). Dado que muchas plataformas globales operan bajo estándares similares en la UE y Reino Unido, el costo de adaptación local es marginal.

Las operadoras de telecomunicaciones asumirán deberes informativos y pondrán a disposición de los abonados las herramientas de control parental existentes, sin intervenir el tráfico ni asumir roles de filtrado de contenidos.

C. Análisis de Beneficios Esperados (Rentabilidad Social)

Impacto positivo sobre la salud mental de niños y adolescentes. Mitigación de conductas adictivas, reducción de cuadros de ansiedad y depresión vinculados al uso problemático

de pantallas, y restauración de hábitos saludables de sueño en la población infantil y adolescente.

Se protegerán mejor los datos personales y la privacidad digital, pues, la iniciativa legislativa propone darle mayor importancia al consentimiento digital (autonomía entre 16 y 18 años; supervisión parental para menores de 16 años), proscripción del perfilamiento comportamental con fines publicitarios dirigidos a menores y minimización de riesgos de ciberacoso y grooming.

Mejora la educación, promoviendo el uso pedagógico seguro de dispositivos en las instituciones educativas bajo la rectoría del MINEDU y desarrollo continuo de la ciudadanía digital en docentes y familias.

Se fortalecerá la eficiencia regulatoria y la seguridad jurídica. Se eliminarán los vacíos normativos mediante la unificación del marco en la Ley 30254 y la canalización de los procedimientos sancionadores bajo la Ley 27444 con criterios de gradualidad y razonabilidad.

MATRIZ DE ANÁLISIS COSTO BENEFICIO Y BALANCE DE IMPACTO

Actor Regulado	**Costos Estimados (criterios conductuales y económicos)**	**Beneficios Directos e Indirectos**	**Balance de impacto**
Niños, Niñas y Adolescentes (NNA)	Restricción gradual voluntaria de entornos no moderados.	Disminución de ciberdelitos, mejora del descanso, protección de datos y salud mental.	**Altamente positivo**
Familias / Padres de Familia	Asunción de un rol activo de orientación y configuración parental (sin sanciones).	Cierre de asimetrías de información, acceso a guías públicas ("Modo Aprendizaje") y acompañamiento.	**Positivo**
Estado / Sector Público	Costos administrativos de reglamentación y adecuación de campañas (*con cargo a presupuesto*).	Reorientación eficiente del canon de espectro, respuesta sanitaria preventiva y reducción de gasto futuro en salud mental.	**Positivo**
Proveedores Digitales (Plataformas/Apps)	Costos de desarrollo de software e interfaz para cumplir estándares por defecto.	Regulación por resultados (sin dictar el *cómo* tecnológico), previsibilidad jurídica y flexibilidad técnica.	**Positivo**

Empresas de Telecomunicaciones	Costo mínimo de mensajería informativa al abonado sobre controles parentales.	Respeto estricto a la neutralidad de red, cero cargas tributarias nuevas y eliminación de bloqueos en red.	**Positivo**

Al haber desestimado las prohibiciones absolutas y las cargas tecnológicas financieramente inviables de la iniciativa original, la propuesta aprobada logra un equilibrio óptimo entre la **protección del interés superior del niño** y la **preservación de la innovación y la neutralidad de red** en el Perú.

X. IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa tiene por finalidad fortalecer el marco jurídico nacional de protección de los derechos de los niños y adolescentes frente a los riesgos asociados a su interacción con los entornos digitales, particularmente aquellos que pueden comprometer su salud mental, privacidad, seguridad y desarrollo integral.

Su incorporación al ordenamiento jurídico permitirá establecer disposiciones específicas sobre prevención del uso problemático de las tecnologías digitales, protección de datos personales, responsabilidades de los proveedores de servicios digitales, orientación a las familias y articulación de las entidades públicas competentes.

La propuesta se sustenta en los principios constitucionales de protección de la persona humana, respeto de su dignidad, tutela de la salud y especial protección de los niños y adolescentes. Asimismo, guarda relación con las disposiciones del Código de los Niños y Adolescentes, la legislación sobre salud mental y el marco jurídico de protección de datos personales.

En particular, la iniciativa contempla modificaciones a la Ley 29733, Ley de Protección de Datos Personales, con el propósito de fortalecer las garantías aplicables al tratamiento de datos personales de niños y adolescentes en entornos digitales, conforme a las disposiciones expresamente previstas en la fórmula legal.

De igual manera, propone la derogación de la Ley 30254, Ley de Promoción para el Uso Seguro y Responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, a fin de sustituir dicho marco por una regulación más amplia que incorpore medidas específicas de protección de la salud mental, bienestar digital y prevención de riesgos.

La iniciativa también articula las competencias de las entidades públicas responsables de la educación, la salud, la protección de poblaciones vulnerables, las telecomunicaciones, la protección de datos personales y la defensa de los consumidores, respetando sus respectivos ámbitos de actuación.

En consecuencia, la entrada en vigor de la norma contribuirá a actualizar y fortalecer el ordenamiento jurídico nacional frente a los desafíos que plantea la creciente participación de los niños y adolescentes en los entornos digitales, mediante un enfoque preventivo, de protección integral y de corresponsabilidad entre el Estado, las familias y los proveedores de servicios digitales.