PROYECTO DE LEY

LEY DE CUIDADO Y BIENESTAR DIGITAL. USO RESPONSABLE DE DISPOSITIVOS Y REDES SOCIALES PARA NIÑAS, NIÑOS Y ADOLESCENTES

CAPITULO I: PRINCIPIOS PARA UNA ARGENTINA DIGITAL SEGURA

Artículo 1°. Objeto. La presente ley tiene como objetivo garantizar el pleno y permanente ejercicio de todos los derechos de las personas menores de edad, garantizando su interés superior y su autonomía progresiva a fin de promover lo establecido en la Ley N° 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes.

Artículo 2°. Marco Normativo de Entornos Digitales Seguros. Establécese el marco normativo para un uso responsable de plataformas de redes sociales y servicios análogos con el fin de proteger a las infancias, las adolescencias y sus familias, promover el bienestar en entornos digitales seguros y responsables, prevenir daños y garantizar mecanismos eficaces de control, reparación y sanción.

Artículo 3°. Principios rectores. La presente ley será interpretada y aplicada de conformidad con los siguientes principios generales vigentes, en consonancia con la Constitución Nacional, la Convención sobre los Derechos del Niño (Ley N° 23.849), la Convención Americana sobre Derechos Humanos (Ley N° 23.054), la Convención sobre los Derechos de las Personas con Discapacidad (Ley N° 26.378), la Ley N° 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes, el Código Civil y Comercial de la Nación, la Ley N° 24.240 de Defensa del Consumidor, la Ley N° 25.326 de Protección de los Datos Personales, la Ley N° 27.078 de Telecomunicaciones (Argentina Digital), y sus normas reglamentarias:

- Interés superior de niñas, niños y adolescentes, y su derecho a ser oídos.
- Autonomía progresiva.
- Accesibilidad y protección especial a menores con discapacidad cognitiva.
- Responsabilidad reforzada de los proveedores.
- Deber de prevención del daño digital y garantía de entornos digitales seguros.
- Diseño seguro, minimización de datos y protección por defecto.
- Privacidad y protección de datos personales.
- Información clara, accesible, veraz y proactiva.
- Deber de colaboración reforzado con el usuario hipervulnerable.
- Acceso equitativo y no discriminación.
- Libertad de expresión.
- Neutralidad tecnológica y adaptabilidad.

Artículo 4°. Responsabilidad reforzada de los proveedores. Todo proveedor de servicios digitales deberá adoptar medidas razonables, proporcionales y efectivas de prevención, seguridad y diseño seguro para proteger los derechos, la privacidad, la integridad, la salud y el desarrollo integral de niñas, niños y adolescentes.

Las plataformas de redes sociales restringidas –X, Instagram, Facebook, YouTube, TikTok y similares– y otros proveedores de servicios en línea –incluyendo servicios de mensajería masiva y comunicación grupal como WhatsApp, Telegram, Discord y similares– tendrán responsabilidad

subjetiva agravada con obligación de prevención, mitigación y reparación de los daños e impactos derivados del uso de sus servicios sobre niñas, niños, adolescentes y sus familias.

Dicha responsabilidad comprende la debida diligencia reforzada en la implementación efectiva y permanente de medidas técnicas, organizativas y operativas destinadas a identificar, prevenir, mitigar y responder a riesgos previsibles derivados del funcionamiento de sus plataformas que puedan afectar a personas menores de edad, tales como el acoso, la agresión, la violencia digital y la explotación digital, el contenido nocivo o no consentido que genere daño y los efectos adictivos, sin que puedan eximirse por el desconocimiento, conductas de terceros o limitaciones tecnológicas.

Ni la responsabilidad parental, ni la del Estado, ni la actuación de terceros por los que no se deba responder, excepto caso fortuito o fuerza mayor, podrán ser invocadas por los proveedores para eludir las obligaciones específicas establecidas en la presente ley. Las obligaciones previstas en la presente ley serán aplicables con independencia de la tecnología utilizada.

Artículo 5°. Prohibición de algoritmos adictivos y explotación digital de menores. Queda prohibido el diseño, utilización o implementación de algoritmos, sistemas automatizados o mecanismos de perfilamiento que empleen datos personales de personas menores de dieciocho (18) años con fines de manipulación comercial, publicidad comportamental, captación compulsiva de la atención, maximización de permanencia, explotación de patrones de vulnerabilidad o inducción de consumos digitales perjudiciales.

Artículo 6°. Publicidad cero para niñas, niños y adolescentes. Queda prohibida la publicidad comercial o promocional dirigida, segmentada, personalizada o amplificada específicamente hacia niñas, niños y adolescentes menores de dieciséis (16) años mediante algoritmos, datos de comportamiento, edad verificada o inferida, geolocalización, intereses, historial de navegación, actividad dentro o fuera de la plataforma, perfiles predictivos o cualquier otro mecanismo de segmentación automatizada en plataformas digitales.

Respecto de adolescentes de dieciséis (16) y diecisiete (17) años, sólo podrá admitirse publicidad comercial o promocional cuando sea lícita, claramente identificable, adecuada a su edad, no discriminatoria, no engañosa, no manipulativa y no basada en datos sensibles, vulnerabilidades, inferencias emocionales, perfiles psicológicos, geolocalización precisa o técnicas de explotación conductual.

En ningún caso podrá dirigirse, segmentarse, recomendarse o amplificarse hacia personas menores de dieciocho (18) años publicidad de productos, servicios o actividades prohibidas, restringidas por edad o perjudiciales para su salud, seguridad, privacidad, integridad, desarrollo o bienestar.

Las plataformas digitales deberán implementar medidas técnicas, organizativas y de moderación para impedir la segmentación publicitaria prohibida, identificar claramente el contenido publicitario o promocional y permitir mecanismos accesibles de denuncia, revisión y limitación de anuncios.

Artículo 7°. Prohibición de publicidad, promoción y patrocinio de juegos de azar y apuestas en entornos digitales. Prohíbase en todo el territorio de la República Argentina la publicidad, promoción y patrocinio, ya sean de carácter público o privado, en todas las plataformas digitales, aplicaciones móviles, redes sociales o servicios de mensajería en línea, de los servicios de juegos de azar y apuestas en línea.

Artículo 8°. Proveedores obligados y ámbito de aplicación. Quedan sujetos a las disposiciones de la presente ley los proveedores de servicios electrónicos accesibles por aplicación o en línea que operen en el país, independientemente de su lugar de constitución o ubicación de sus servidores, cuando sus servicios, de manera directa o indirecta, se encuentren dirigidos o sean utilizados por usuarios ubicados en la República Argentina, o produzcan efectos en el territorio nacional.

El servicio se considera dirigido a usuarios ubicados en la República Argentina cuando, entre otros elementos, ofrece publicidad o monetización, dispone condiciones comerciales aplicables dirigidas a usuarios locales, utiliza idioma español orientado al mercado local, registra una cantidad significativa de usuarios en el territorio nacional o realiza tratamiento sistemático de datos de personas ubicadas en el país.

Se entiende por proveedores obligados tanto a aquellos que brindan servicios mediante plataformas de redes cuyo propósito principal o relevante sea permitir la interacción social entre múltiples usuarios, la publicación de contenidos y/o el establecimiento de vínculos entre perfiles; como a los que operan a través de servicios de mensajería o comunicación de amplio alcance que permiten la creación de grupos, canales, comunidades o espacios de interacción con múltiples usuarios simultáneos y funcionalidades de difusión masiva de contenidos.

Quedan excluidos los servicios cuya finalidad principal sea educativa, sanitaria, laboral, administrativa o de mensajería privada interpersonal, siempre que no incorporen funcionalidades de red social abierta, recomendación algorítmica personalizada, difusión masiva de contenidos, canales o comunidades abiertas, transmisiones en vivo, perfiles públicos o contacto irrestricto con terceros.

Artículo 9°. Fijación de sede y representación legal en la República Argentina. Los proveedores extranjeros deberán:

1. Establecer sucursal o establecimiento permanente en los términos de la Ley General de Sociedades N° 19.550 o, en caso de tratarse de una persona jurídica no societaria, inscribirse en el Registro Público que corresponda;
2. Constituir domicilio en el territorio nacional dentro de los noventa (90) días corridos de la entrada en vigencia de la presente ley o desde el inicio de sus operaciones en el país;
3. Registrar dicho domicilio ante la autoridad de aplicación, con actualización obligatoria ante cualquier modificación, en un plazo máximo de cinco (5) días hábiles;
4. Designar representantes legales titular y alterno, personas humanas con domicilio en el país, con facultades suficientes para responder ante requerimientos judiciales y administrativos, recibir notificaciones con validez legal, representar al proveedor ante todos los organismos del Estado y cumplir con las medidas que ordenare la autoridad de aplicación;
5. Registrar dichos representantes ante la autoridad de aplicación, con actualización obligatoria ante cualquier modificación, en un plazo máximo de cinco (5) días hábiles; y
6. Publicar de forma visible en sus plataformas, interfaces y sitios web los datos del domicilio legal en la República Argentina y de contacto de los representantes locales designados.

El incumplimiento de estas obligaciones constituirá una infracción gravísima, pudiendo disponerse el bloqueo de acceso al servicio en todo el territorio nacional. La carga de acreditar su cumplimiento recaerá sobre el proveedor.

Los representantes legales designados tendrán responsabilidad personal cuando mediare dolo o culpa grave, y responderán por los daños previsibles derivados de la exposición al riesgo creado por los servicios de los proveedores, excepto que acrediten haber adoptado todas las medidas de prevención razonables conforme al estado de la técnica, la normativa vigente y los principios de debida diligencia digital.

Artículo 10°. La salud digital como interés público. Declárase de interés público nacional la protección de la salud mental, el bienestar, la privacidad, la seguridad, la autonomía progresiva y el desarrollo integral de niñas, niños y adolescentes en entornos digitales, frente a diseños, funcionalidades, sistemas de recomendación o modelos de explotación económica que generen riesgos previsibles de uso compulsivo, exposición nociva, captación abusiva de la atención o

afectación conductual o cognitiva significativa. En particular se priorizará proteger e incrementar, en lo posible, la:

- **Atención humana:** es decir, la aptitud de la persona menor de edad para seleccionar y sostener voluntariamente su foco cognitivo frente a estímulos relevantes, en condiciones compatibles con su desarrollo, aprendizaje y bienestar;
- **Autonomía conductual digital:** definida como la capacidad de la persona menor de edad para tomar decisiones informadas y conscientes, acordes a su edad y madurez, con relación a su comportamiento y tiempo de permanencia en entornos digitales, sin manipulación indebida;
- **Prevención de patrones de uso intensivo:** entendidos como perjudiciales cuando interfieren de modo relevante con el descanso, la educación, la sociabilidad, la salud mental o el desarrollo integral de la persona menor de edad.

Artículo 11°. Requisito de matrícula profesional vigente. Cuando se trate de publicaciones, videos o contenidos similares que contengan recomendaciones, diagnósticos, tratamientos o exposiciones con contenido médico sobre salud mental u otras actividades que afecten el bienestar general y la salud pública, las empresas de redes sociales y plataformas digitales deberán restringir su visualización a menores de dieciocho (18) años, salvo que se exhiba de forma visible, inequívoca y constatable el nombre completo del profesional y su respectiva matrícula habilitante vigente.

Artículo 12°. Prohibición de uso en el ámbito escolar. Queda prohibido el uso de los servicios suministrados por los proveedores, así como la utilización de teléfonos celulares y otros dispositivos digitales personales en el ámbito escolar, en los tres niveles de la educación obligatoria conforme se establece en la Ley N° 26.206, tanto a estudiantes como a docentes, durante el horario de clases, excepto:

1. Cuando se utilizaren con fines pedagógicos, mediados por el/la docente, debidamente articulados con un contenido curricular y con un tiempo de uso predeterminado; o
2. Con finalidad formativa, mediados por el/la docente, para enseñar sobre su uso adecuado, capacitar en pautas de seguridad y en la prevención de los riesgos asociados, o reflexionar críticamente sobre el entorno digital, con una duración limitada a la actividad programada.

Queda exceptuado de la prohibición el uso que requieran personas con discapacidad o con una necesidad transitoria excepcional, con el objeto de asegurar su accesibilidad, siempre que sea condición indispensable y efectiva para el proceso de aprendizaje.

Las instituciones educativas deberán establecer pautas claras, proporcionales y no discriminatorias para la guarda, uso, autorización, supervisión y eventual retiro temporal de dispositivos digitales personales, evitando medidas arbitrarias o que vulneren la privacidad, la dignidad o los derechos de niños, niñas y adolescentes.

La reglamentación de esta disposición y su control de aplicación estará a cargo de las provincias y de la Ciudad Autónoma de Buenos Aires en el ámbito de sus competencias, de las universidades nacionales o del Estado Nacional, conforme a quien tenga a su cargo las respectivas unidades educativas.

Artículo 13°. Entorno digital de riesgo. Se considera configurado el entorno de riesgo en un servicio, plataforma, aplicación o sistema digital, en relación con personas menores de edad, cuando presente una o más de las siguientes características estructurales, funcionales o de diseño susceptibles de afectar su salud, desarrollo integral, seguridad o bienestar:

- **Diseño conductual dependiente:** incorporación de mecanismos orientados a prolongar artificialmente el tiempo de uso o que generen conductas de uso compulsivo, tales como

navegación continua sin interrupciones significativas, reproducción automática de contenidos, patrones oscuros o sistemas de notificación intrusiva orientados a incentivar el reingreso frecuente.

- **Algoritmos opacos:** utilización de sistemas de recomendación que prioricen contenidos para maximizar la permanencia del usuario menor de edad sin criterios de transparencia, o funcionalidades que faciliten la difusión masiva o viralización de contenidos sin mecanismos de control de exposición progresiva o con recompensas variables diseñadas para la retención.
- **Interacción social irrestricta:** posibilidad de contacto con terceros sin verificación adecuada de identidad o edad, o sin mecanismos efectivos de filtrado y prevención de conductas abusivas.
- **Exposición a contenidos problemáticos:** recomendación, distribución o acceso a contenidos inadecuados para la edad del usuario, incluyendo aquellos que promuevan violencia, conductas peligrosas, autolesiones, suicidio o resulten incompatibles con la protección integral del menor.
- **Insuficiencia de medidas de mitigación:** ausencia o ineficacia de herramientas de control, advertencias, límites de uso o mecanismos de interrupción orientados a la protección del menor.

Artículo 14°. Calificación del riesgo. La concurrencia de una o más características estructurales, funcionales o de diseño que configuran un entorno digital de riesgo serán calificadas, conforme a su intensidad, reiteración, capacidad de daño y ausencia de mitigación, en:

- **Riesgo leve:** cuando los elementos se presenten de manera aislada, con bajo impacto potencial y existan mecanismos de mitigación accesibles, efectivos y fácilmente configurables por parte del usuario o sus responsables legales.
- **Riesgo moderado:** cuando los elementos se presenten de manera persistente o combinada, con un impacto definitivo en los hábitos de uso o exposición del menor, y los mecanismos de mitigación resulten limitados, de difícil acceso o insuficientes.
- **Riesgo alto o crítico:** cuando los elementos se encuentren integrados en el diseño estructural del servicio o plataforma, generen incentivos conductuales intensivos o exposición sistemática a situaciones potencialmente dañinas, y exista ausencia o ineficacia sustancial de medidas de mitigación.

La autoridad de aplicación podrá, conforme a criterios técnicos verificables, establecer estándares complementarios para la identificación, medición y evaluación de los niveles de riesgo, de acuerdo con la evolución tecnológica y los parámetros internacionales aplicables.

CAPÍTULO II. CONDICIONES DE ACCESO, ENTORNO DIGITAL SALUDABLE Y PREVENCIÓN DE DAÑOS

Artículo 15°. Edades de acceso. Los proveedores implementarán las medidas técnicas necesarias a fin de que toda persona humana menor de dieciocho (18) años, independientemente de la edad declarada al momento del registro en una plataforma de red social restringida, encuadre, progresivamente, en las siguientes categorías:

- **Prohibición absoluta:** Queda prohibido a los proveedores permitir la creación o mantenimiento de cuentas de personas menores de catorce (14) años de edad en plataformas de redes sociales restringidas. El consentimiento de los progenitores o representantes legales no será suficiente para exceptuar esta prohibición.
- **Acceso restringido:** El acceso a la creación o mantenimiento de cuentas de usuarios entre catorce (14) años de edad cumplidos y menores de dieciséis (16) años de edad requerirá la previa autorización parental; se vinculará el perfil a la cuenta del adulto responsable, se aplicarán mecanismos de privacidad reforzada por defecto, mensajería limitada a contactos

vinculados, desactivación de geolocalización, prohibición de publicidad comportamental y limitación de sistemas de recomendación personalizados orientados a maximizar la permanencia.

- **Acceso condicionado:** A partir de los dieciséis (16) años de edad cumplidos y hasta la mayoría de edad, podrán registrarse conforme a configuraciones reforzadas de protección por defecto y recibiendo información clara y completa adecuada al grado de madurez del usuario. Deberán preverse mecanismos de intervención parental proporcionales, incluyendo la posibilidad de que progenitores o representantes legales puedan formular oposición al registro, así como el derecho a solicitar restricciones en caso de riesgo acreditado, conforme lo establezca la reglamentación.

Artículo 16°. Herramientas de supervisión familiar. Reportes de seguimiento. Los proveedores pondrán a disposición, en todos los casos, recursos de control parental y funciones nativas de emparejamiento familiar que permitan la administración de permisos, limitación de tiempos de uso en los dispositivos, filtro de contenidos, bloqueo y autorización de descarga de aplicaciones y envío de reportes automáticos a los adultos responsables con periodicidad mensual, conforme al criterio de progresividad y sin afectar la privacidad, intimidad, libre expresión y desarrollo autónomo del usuario menor de edad. Excepcionalmente podrán establecerse, cuando exista riesgo razonablemente acreditado, mecanismos de control y revisión del historial de uso.

Artículo 17°. Garantías para el usuario adolescente. En resguardo de los derechos del adolescente usuario, los proveedores deberán garantizarles el acceso a información adecuada, completa y veraz; a instancias de revisión de decisiones automatizadas; a un mecanismo de impugnación de bloqueo por error; y asegurar con medidas efectivas los derechos a la privacidad, no discriminación, accesibilidad y a no ser sometidos a perfilamiento comercial.

Artículo 18°. Sistema de verificación técnica de edad. Los proveedores implementarán procedimientos técnicos, documentados, eficaces y proporcionales al nivel de riesgo del servicio, destinados a verificar la edad en el proceso de registro de usuarios para asegurar la efectividad de las restricciones, garantizando el respeto por la privacidad y la protección de datos personales, conforme a los siguientes estándares:

1. Excluir la mera autodeclaración como único mecanismo;
2. Utilizar al menos dos (2) métodos de verificación reconocidos y complementarios;
3. Garantizar que los datos utilizados para la verificación no sean almacenados más allá del tiempo estrictamente necesario para completar el proceso;
4. Implementar controles periódicos de reverificación de edad, con una frecuencia mínima de doce (12) meses para cuentas de usuarios cuya edad sea cercana a los límites establecidos;
5. Aplicar controles adicionales de detección de evasión o de intentos de elusión de los mecanismos de verificación de edad;
6. Prevenir el uso indebido de identidad etaria, entendida como la conducta consistente en declarar, registrar o utilizar una edad distinta a la real con el fin de eludir las restricciones establecidas en la presente ley.

El incumplimiento de estos deberes será considerado como una infracción grave. La falta de implementación de mecanismos de verificación interoperables con los sistemas definidos por la autoridad de aplicación impedirá la prestación del servicio en el territorio nacional.

Artículo 19°. Protección de datos de verificación. Los datos obtenidos exclusivamente para la verificación de edad deberán ser destruidos de forma inmediata una vez cumplimentado el proceso, prohibiéndose su uso para cualquier finalidad comercial o de seguimiento, sin posibilidad de reutilización, tratamiento ulterior ni cesión.

Artículo 20°. Protocolo de "prueba de edad". La autoridad de aplicación reglamentará un protocolo de consulta en el cual el Estado Nacional solo responda con un valor booleano (Verdadero-Falso) ante la pregunta de si el usuario supera el umbral de edad establecido.

En ningún caso el Estado Nacional transferirá a las empresas privadas el número de Documento Nacional de Identidad, domicilio, imagen biométrica o fecha exacta de nacimiento del solicitante.

El acceso a esta consulta de validación de edad para los fines de cumplimiento de esta ley, siempre que se realice a través de un servicio estatal, será gratuito.

El resultado de la consulta no podrá ser utilizado para fines distintos del cumplimiento de la presente ley.

Artículo 21°. Alternativas de verificación para usuarios extranjeros. En caso de usuarios extranjeros residentes en el país que no posean Documento Nacional de Identidad, o ante fallas sistémicas, se admitirán herramientas automatizadas de estimación o verificación etaria, empleando métodos de análisis de rasgos sin almacenamiento de imagen o sobre la base de comprobación de documentos de viaje.

Las herramientas y métodos automatizados de estimación etaria deberán ser proporcionales, no discriminatorios, explicables en términos generales, estar sometidos a evaluación de impacto en protección de datos, contar con mecanismos de revisión o impugnación por parte del usuario y estar sujetos a la auditoría anual de la autoridad de aplicación.

Artículo 22°. Configuración de privacidad protectora por defecto. Los perfiles de usuarios menores de edad deberán configurarse por defecto con el máximo nivel de privacidad, adoptando los siguientes parámetros:

- **Geolocalización:** desactivación por defecto de la ubicación en tiempo real, la cual sólo podrá admitirse respecto de adultos responsables de manera expresa, revocable, proporcionada, informada y visible para el usuario menor de edad, conforme a su edad y grado de madurez.
- **Privacidad:** visibilidad del contenido publicado solo para contactos aprobados.
- **Prohibición de indexación:** inhabilitación de la indexación en motores de búsqueda externos.
- **Limitación de recomendación algorítmica:** los perfiles y contenidos publicados por usuarios menores de edad no deberán ser recomendados, sugeridos o amplificados algorítmicamente hacia usuarios no vinculados.
- **Etiquetado, menciones y reconocimiento de imagen:** Toda etiqueta o mención deberá requerir previa autorización del usuario menor de edad y/o de adulto responsable.
- **Visibilización de estado y actividad:** la visibilización del estado en línea, última conexión, actividad reciente y/o demás señales de disponibilidad o presencia digital del usuario menor de edad deberá encontrarse desactivada por defecto o limitada a contactos aprobados y verificados.
- **Incorporación a grupos, comunidades o canales:** la participación del usuario menor de edad en grupos, comunidades, canales, listas de difusión, entre otros, deberá requerir autorización expresa y contar con mecanismos claros de salida, bloqueo y denuncia.

Artículo 23°. Identificación verificada para contactar a menores y limitación de Mensajería Directa. Los proveedores de servicios de internet y aplicaciones de interacción social deberán implementar mecanismos de restricción en sus sistemas de mensajería directa para cuentas de usuarios menores de edad. La recepción de comunicaciones quedará limitada exclusivamente a los perfiles que el menor haya admitido previamente en su lista de contactos y, tratándose de remitentes que cuenten con una validación de identidad fehaciente y perfil verificado.

Artículo 24°. Deber de información adecuada a la edad de niñas, niños y adolescentes. Los proveedores deberán informar de manera clara, accesible, previa y comprensible a los usuarios menores de edad y, en su caso, a sus progenitores o representantes legales:

1. Los riesgos asociados al uso de redes sociales, incluyendo los relativos a la salud mental, exposición a contenidos inapropiados y dinámicas de uso compulsivo;
2. Las configuraciones de privacidad aplicables; y
3. Los mecanismos de denuncia y asistencia disponibles.

Dicha información deberá presentarse en lenguaje claro, accesible y adaptado a la edad y grado de madurez de la persona usuaria menor de edad.

Artículo 25°. Protección reforzada frente a sistemas de Inteligencia Artificial y algoritmos de manipulación digital. Los proveedores de plataformas digitales, motores de recomendación, asistentes virtuales, sistemas automatizados de interacción o cualquier otro servicio digital que utilice Inteligencia Artificial o procesamiento algorítmico respecto de usuarios menores de dieciocho (18) años serán responsables de garantizar el interés superior del niño, la protección de la salud mental, su desarrollo integral y su autonomía progresiva.

Artículo 26°. Filtros de seguridad inmediata y bloqueo de contenido dañino en búsquedas asistidas por Inteligencia Artificial. Las búsquedas asistidas por Inteligencia Artificial y los entornos conversacionales automáticos deberán integrar de forma nativa filtros de seguridad eficaces, proporcionales y actualizados que impidan la generación, difusión o facilitación de respuestas de texto, imágenes o códigos que puedan inducir daño a las niñas, niños y adolescentes. Esto incluye, de manera taxativa, búsquedas o consultas orientadas a:

- Protocolos de autolesión, ideación suicida o trastornos de la conducta alimentaria;
- Dinámicas o plataformas de juegos de azar, apuestas en línea o esquemas de monetización compulsiva para menores de edad;
- Contenidos de carácter por pornográfico, hipersexualizado o que promuevan la explotación sexual infantil; y
- Contenidos que promuevan la violencia, conductas peligrosas o ciberacoso.

El incumplimiento de esto será considerado una infracción gravísima en los términos de la presente ley.

Artículo 27°. Protocolo Automático de Gestión, Alerta y Derivación Asistida ante Crisis de Inteligencia Artificial. Cuando los sistemas de Inteligencia Artificial detecten consultas o patrones de interacción que reflejen un riesgo crítico para la vida, integridad o salud mental del menor, el entorno digital interrumpirá la respuesta estándar y deberá de forma obligatoria e inmediata:

1. Bloquear la entrega de información que profundice la situación de riesgo;
2. Exhibir en la interfaz principal recursos institucionales de ayuda en crisis y líneas de asistencia gratuita legibles y adaptadas a la madurez cognitiva del usuario;
3. Notificar, de manera confidencial y resguardando la privacidad del menor, a las cuentas de adultos responsables vinculadas mediante las herramientas de supervisión familiar y;
4. Notificar a la Autoridad de Aplicación ante un evento crítico con el fin de tener un control de auditoría que mejore el sistema, rendición de cuentas y cumplimiento legal.

El incumplimiento de estos deberes será considerado una infracción gravísima a los efectos sancionatorios de la presente ley.

Artículo 28°. Prevención y alertas frente al uso problemático, compulsivo o perjudicial. Los proveedores, observando la normativa de protección de datos personales, implementarán sistemas

automatizados de detección de patrones de uso intensivo, persistente o con pérdida de control sobre el tiempo de uso, conforme a los siguientes parámetros:

- Emisión de alertas claras, visibles y comprensibles al usuario cuando se verifiquen dichos patrones, incluyendo: tiempo acumulado de uso, frecuencia de conexión, recomendación de pausa y/o desconexión.
- Eliminación de funcionalidades que incentiven conductas adictivas tales como: reproducción automática infinita, sistemas de recompensas variables y notificaciones diseñadas para maximizar la permanencia continua.
- Implementación de mecanismos que impidan que los menores de edad accedan a contenidos médicos, sobre salud mental u otras actividades reguladas sin previa verificación de la matrícula habilitante exhibida de forma visible.
- Prohibición del uso de inferencias, métricas o datos derivados de estos sistemas con fines publicitarios, comerciales, de perfilamiento, recomendación de contenidos o maximización de permanencia, sujetándose a los principios de minimización, finalidad específica, seguridad y auditoría.

El incumplimiento de estos deberes será considerado una infracción grave en los términos de la presente ley.

Artículo 29°. Protección en entornos de videojuegos y plataformas de juego en línea. Los proveedores de videojuegos en línea, plataformas de interacción lúdica digital, servicios de gaming, aplicaciones de juego multijugador, mundos virtuales interactivos y cualquier otro entorno digital destinado total o parcialmente a personas menores de dieciocho (18) años deberán adoptar medidas específicas de protección integral de derechos, prevención de conductas adictivas y resguardo de la salud mental y emocional de niños, niñas y adolescentes.

Artículo 30°. Prohibiciones en entornos de videojuegos y plataformas de juego en línea. Los proveedores enumerados en el artículo precedente tendrán prohibido:

1. El diseño o utilización de mecánicas destinadas a incentivar compulsivamente la permanencia continua, la conexión prolongada o la reiteración sistemática de consumo mediante recompensas variables, estímulos psicológicos de dependencia o mecanismos equivalentes de manipulación conductual;
2. La incorporación de sistemas de monetización dirigidos a menores de edad que promuevan compras impulsivas, microtransacciones reiteradas, cajas de recompensa aleatoria, premios probabilísticos o mecanismos análogos que reproduzcan lógicas asimilables a los juegos de azar;
3. La utilización de perfiles algorítmicos destinados a identificar vulnerabilidades emocionales, patrones de conducta compulsiva o hábitos de consumo de menores de edad para maximizar ingresos, permanencia o interacción;
4. La utilización de sistemas automatizados que recomienden contenidos violentos, autodestructivos, sexualizados, discriminatorios o inapropiados para la edad del usuario y;
5. Dificultar de manera injustificada la desactivación de funciones sociales, la limitación de compras, la cancelación de suscripciones, la eliminación de datos, el bloqueo de usuarios, la denuncia de conductas abusivas o el ejercicio de derechos por parte del usuario menor de edad y/o sus adultos responsables.

El incumplimiento de estos deberes será considerado una infracción gravísima en los términos de la presente ley.

Artículo 31°. Control de apuestas en plataformas de pago digitales para usuarios menores de edad. Las entidades financieras, billeteras virtuales, bancarias y las empresas de cobros o servicios de pago autorizadas por el Banco Central de la República Argentina (BCRA) que ofrecen cuentas

de pago para usuarios menores de edad, deberán implementar de forma obligatoria sistemas automatizados de filtrado, control y detección temprana de transacciones destinadas a plataformas digitales de juego y apuestas en línea.

Ante la detección de dichos indicadores, deberán:

1. Restringir de manera automática cualquier transferencia, pago o consumo dirigido a sitios de apuestas y/o juegos de azar en línea;
2. Activar alertas por reiteración de consumos digitales a través de un monitoreo que identifique patrones de transacciones reiteradas que denoten conducta compulsiva y/o ludopatía;
3. Ante la detección de patrones sospechosos la billetera virtual deberá notificar de inmediato a los progenitores, adultos responsables y/o tutores asignados a la cuenta del usuario menor de edad vinculada a la cuenta, procediendo a la suspensión preventiva de los pagos hasta que medie ratificación expresa de los mismos.

El incumplimiento de cualquiera de estas obligaciones será considerado una infracción gravísima según la entidad del daño provocado u omitido

Artículo 32°. Prevención obligatoria de daños críticos. Los proveedores deberán implementar, de forma obligatoria y permanente, protocolos específicos de detección temprana, intervención y derivación asistida frente a situaciones consideradas de riesgo crítico para niñas, niños y adolescentes, tales como la prevención del suicidio; advertencia de conductas adictivas digitales como la ludopatía; prevención y erradicación del ciberacoso; prevención de la autolesión; explotación sexual infantil y advertencia de trastornos de la conducta alimentaria.

Ante la detección de dichos indicadores, deberán:

1. Interrumpir o limitar la difusión del contenido;
2. Mostrar de forma inmediata recursos de ayuda en crisis adecuados a la edad y accesibles desde la misma interfaz;
3. Notificar de forma confidencial y proporcional a los adultos responsables vinculados.

El incumplimiento de cualquiera de estas obligaciones será considerado una infracción gravísima según la entidad del daño provocado u omitido.

Artículo 33°. Verificación de edad para el acceso a contenidos aptos exclusivamente para mayores de edad. Los proveedores de servicios de plataformas digitales, sitios web o aplicaciones móviles que alojen, difundan o comercialicen contenidos de carácter pornográfico deberán implementar un sistema obligatorio, previo y eficaz de verificación de edad que impida de forma absoluta el acceso a personas menores de dieciocho (18) años.

El incumplimiento de esta obligación será considerado una infracción gravísima según la entidad del daño provocado u omitido.

CAPÍTULO III. AUTORIDAD DE APLICACIÓN, DEBER DE INFORMACIÓN Y RÉGIMEN DE PROMOCIÓN DE LA SALUD DIGITAL

Artículo 34°. Autoridad de aplicación. La autoridad de aplicación será la Agencia de Acceso a la Información Pública (AAIP), o el organismo que en el futuro la reemplace, en coordinación con la Defensoría de los Derechos de las Niñas, Niños y Adolescentes.

La autoridad de aplicación deberá:

- Supervisar el cumplimiento de las disposiciones de esta ley.
- Recibir y tramitar denuncias de usuarios, familias y organizaciones de la sociedad civil.
- Imponer sanciones administrativas, garantizando el debido proceso administrativo conforme a lo establecido en la presente ley.
- Conducir estudios y evaluaciones de impacto, llevar un registro de métricas sobre la base de la información provista por los proveedores y la recolectada mediante auditorías independientes.
- Elaborar y publicar un informe anual sobre el estado de la protección de menores en entornos digitales, que remitirá al Congreso de la Nación antes de su publicación.
- Establecer un protocolo de actuación rápida, en conjunto con el Ministerio Público Fiscal, frente a presuntos casos de grooming, abuso o explotación sexual infantil.
- Consultar y cooperar, entre otros, con la Secretaría Nacional de Niñez, Adolescencia y Familia (o el organismo de rango equivalente que la sustituya), con el Ente Nacional de Comunicaciones (ENACOM) –o el organismo que en el futuro lo reemplace–, y con los organismos de defensa y protección de los consumidores, de salud mental y de protección de datos personales.

Artículo 35°. Responsabilidad concurrente del Estado. La protección de las personas menores de edad en entornos digitales constituye una responsabilidad concurrente del Estado y de los proveedores, sin perjuicio de las responsabilidades específicas establecidas en el presente régimen. El Estado deberá garantizar en sus políticas públicas:

- Regulación y fiscalización adecuadas y proporcionales;
- Educación y ciudadanía digital, y formación y capacitación docente;
- Planes y programas de prevención de riesgos y de asistencia en materia de salud digital infantil;
- Canales accesibles de denuncia y asistencia;
- Acompañamiento y guía para las familias;
- Adecuada protección de datos personales.

La responsabilidad parental, entendida como el conjunto de deberes y derechos de los progenitores o adultos responsables conforme al Código Civil y Comercial de la Nación, no exime ni reduce las obligaciones propias del Estado ni de los proveedores de servicios digitales conforme se prevé en la presente ley.

Artículo 36°. Informe obligatorio ante el Poder Legislativo. Los proveedores presentarán ante el Congreso de la Nación, por Mesa de Entradas de ambas cámaras, y ante la autoridad de aplicación, con carácter obligatorio y periodicidad semestral, un informe público de transparencia que contendrá, como mínimo:

- **Análisis estadístico del período:** con datos actualizados sobre la cantidad de usuarios menores de edad activos en el país, segmentados por rango etario; volumen y tipología de contenidos eliminados, reportados o restringidos por razones de protección de menores; cantidad de cuentas suspendidas o bloqueadas por violación de las normas de edad; e incidentes de grooming, ciberacoso, contenido de abuso sexual infantil u otras situaciones críticas detectadas y gestionadas.
- **Estado de implementación de las medidas de protección:** con detalle del cumplimiento de las obligaciones establecidas por la presente ley, indicando los sistemas de verificación de edad en operación, las herramientas de control parental disponibles, los protocolos de respuesta ante situaciones de riesgo, las acciones de moderación de contenidos aplicadas y los mecanismos de prevención de uso problemático, compulsivo o perjudicial o de daños críticos implementados.

- **Evaluación de efectividad:** sobre la base de un análisis crítico del impacto de las medidas implementadas, incluyendo indicadores de reducción de riesgo, tiempos de respuesta ante incidentes, índices de satisfacción de usuarios y familias, y métricas de bienestar digital.
- **Plan de mejora para el próximo período:** indicando compromisos específicos, medibles y un cronograma definido para la mejora de las medidas de protección implementadas.
- **Recomendaciones normativas y regulatorias:** tanto para la autoridad de aplicación como para el Poder Legislativo, en su caso con propuestas concretas y fundadas para mejorar el marco regulatorio vigente, incluyendo sugerencias sobre nuevas medidas de protección, actualizaciones tecnológicas necesarias, identificación de vacíos normativos y estándares internacionales comparados que pudieran adoptarse en la República Argentina.

Los informes recibidos se publicarán en los sitios oficiales del Congreso de la Nación, de la autoridad de aplicación y de los proveedores. Las comisiones parlamentarias competentes en la temática de niñez, adolescencia y familia de cada cámara y/o la Comisión Bicameral de la Ley N° 26.061 podrán convocar, al menos una (1) vez por año, a audiencia pública a los representantes de los principales proveedores para la presentación y debate de dichos informes.

La omisión, presentación extemporánea o presentación con datos incompletos, falsos o engañosos de este informe constituirá una infracción grave. La reiteración de la conducta o la presentación manifiestamente fraudulenta constituirá una infracción gravísima.

Artículo 37°. Promoción de la Salud Digital. Créase el Fondo de Promoción de la Salud Digital (FPSD), destinado a financiar programas conforme con la responsabilidad del Estado Nacional establecida en el artículo 34, el cual se ifnanciará con lo recaudado en el Régimen Sancionatorio y la Tasa de Prevención Digital establecidas en la presente ley.

El Fondo será administrado por la autoridad que determine la reglamentación, con control presupuestario, rendición pública anual e intervención de los organismos competentes en niñez, salud y educación.

Estos recursos se aplicarán para:

- Desarrollar herramientas tecnológicas de bienestar digital.
- Implementar instancias de promoción de la salud mental y prevención de adicciones conductuales generadas por el uso de redes sociales y dispositivos electrónicos.
- Realizar campañas de concientización sobre el uso responsable dirigidas a menores, progenitores y establecimientos educativos.
- Financiar investigaciones sobre el impacto de las plataformas digitales en la salud de niñas, niños y adolescentes.
- Sostener líneas de asistencia gratuita para usuarios menores de edad que sean víctimas del mal uso de las plataformas de redes sociales restringidas y proveedores de servicios en línea.

Artículo 38°. Tasa de Prevención Digital: contribución por los daños al bienestar infantil. Establécese la Tasa de Prevención Digital (TPD), de carácter anual, a cargo de los proveedores obligados por la presente ley, destinada a financiar las acciones estatales de mitigación del riesgo creado y de concientización respecto de los daños previsibles que sus modelos de negocio, diseños de interfaz y sistemas algorítmicos generen en el bienestar físico, mental y emocional de las personas menores de edad usuarias en la República Argentina.

Esta tasa se liquidará mediante declaración jurada anual presentada ante la autoridad de aplicación dentro de los noventa (90) días corridos contados a partir del cierre de cada ejercicio económico del proveedor, calculándose bajo la siguiente modalidad:

- **a) Tasa base:** Equivalente al cero coma dos por ciento (0,2%) de la facturación comercial anual del proveedor o grupo económico controlante obtenida por operaciones dentro del territorio de la República Argentina.
- **b) Ajuste por nivel de riesgo:** La tasa base se incrementará en un cincuenta por ciento (50%) para aquellos proveedores cuyos entornos sean calificados con riesgo moderado, y en un cien por ciento (100%) para aquellos proveedores calificados con riesgo alto o crítico, conforme a la clasificación técnica prevista en los artículos 13 y 14 de esta ley.
- **c) Reducción por cumplimiento proactivo:** Los proveedores que acrediten de manera fehaciente, mediante auditoría independiente homologada por la autoridad de aplicación, la implementación efectiva y superadora de las medidas de protección exigidas por esta ley podrán acceder a una reducción de hasta el treinta por ciento (30%) de la tasa liquidada.

Los fondos recaudados en virtud de esta tasa serán transferidos de forma íntegra y directa al Fondo de Promoción de la Salud Digital (FPSD) creado por el artículo 36.

La omisión de la presentación de la declaración jurada o su confección con datos falsos o adulterados constituirá una infracción gravísima, habilitando la aplicación de las sanciones máximas previstas en esta norma, sin perjuicio de las acciones penales que pudieren corresponder por falsedad documental o fraude.

CAPÍTULO IV. RÉGIMEN DE RESPONSABILIDAD Y SANCIONATORIO Y DISPOSICIONES COMPLEMENTARIAS

Artículo 39°. Régimen progresivo de sanciones. El incumplimiento de los proveedores a las obligaciones establecidas en la presente ley los hará pasibles de las siguientes sanciones, sin perjuicio de otras responsabilidades civiles, penales o administrativas que pudieren corresponder:

1. Apercibimiento.
2. Implementación obligatoria de medidas correctivas, auditorías externas independientes o planes de adecuación bajo supervisión de la autoridad de aplicación.
3. Multa de entre el cero coma dos por ciento (0,2%) y el cinco por ciento (5%) de la facturación global anual correspondiente al ejercicio económico anterior, entendiendo por tal los ingresos brutos consolidados del proveedor infractor o del grupo económico propietario o controlante, si lo hubiere, que corresponda al último ejercicio económico anual cerrado.
4. Suspensión temporal de actividades publicitarias o comerciales vinculadas al servicio en el territorio nacional por el plazo máximo de noventa (90) días.
5. Limitación, restricción o suspensión parcial de funcionalidades del servicio en el territorio nacional.
6. Bloqueo de acceso al servicio en todo el territorio nacional.

Las sanciones podrán aplicarse de manera independiente o conjunta, conforme a la gravedad de la infracción y de acuerdo con los criterios de graduación establecidos en la presente ley.

Artículo 40°. De las infracciones e incumplimientos. Las infracciones se clasifican en leves, moderadas, graves, muy graves y gravísimas, conforme a la naturaleza del incumplimiento, el nivel de riesgo generado, la afectación de derechos de personas menores de edad, la reiteración de la conducta y el grado de incumplimiento de los deberes establecidos por esta ley. Se considerarán como:

- **Infracciones leves:** incumplimientos formales, aislados o de bajo impacto que no generen un riesgo significativo para las personas menores de edad, incluyendo retrasos menores en la adecuación de términos y condiciones, defectos puntuales de información o fallas no sistémicas en configuraciones protectoras por defecto. Serán sancionadas con

apercibimiento o multa de entre el cero coma dos por ciento (0,2%) y el uno por ciento (1%) de la facturación global anual.

- **Infracciones moderadas:** incumplimientos parciales o deficientes de las obligaciones previstas en la presente ley que, sin generar daño masivo o estructural, afecten la eficacia del régimen de protección, incluyendo: la implementación incompleta o deficiente de mecanismos de verificación de edad; fallas en la obtención o validación del consentimiento parental, cuando correspondiere; configuraciones de privacidad que no cumplan estándares mínimos; o la falta de mecanismos efectivos de denuncia o asistencia. Serán sancionadas con multa de entre el uno por ciento (1%) y el dos por ciento (2%) de la facturación global anual, pudiendo disponerse adicionalmente la restricción parcial de funcionalidades.
- **Infracciones graves:** incumplimientos que generen un riesgo significativo o afecten de manera relevante los derechos, la privacidad, la seguridad, la salud mental o el desarrollo integral de personas menores de edad, incluyendo: la ausencia de mecanismos efectivos de verificación de edad; el uso indebido de datos personales de personas menores de edad; el incumplimiento de configuraciones protectoras por defecto; la falta de adopción de medidas frente a entornos digitales de riesgo; el incumplimiento del deber de debida diligencia digital; o la omisión de mecanismos razonables de prevención, detección o mitigación de situaciones de acoso, grooming o contacto inapropiado entre usuarios menores de edad. Serán sancionadas con multa de entre el dos por ciento (2%) y el tres por ciento (3%) de la facturación global anual, pudiendo disponerse la restricción de funcionalidades, suspensión de actividades publicitarias o auditorías obligatorias.
- **Infracciones muy graves:** incumplimientos estructurales, reiterados o de alto impacto que impliquen una vulneración de los derechos de personas menores de edad, incluyendo: el diseño o mantenimiento de sistemas orientados a fomentar el uso compulsivo; la utilización de algoritmos dirigidos a maximizar el tiempo de permanencia sin medidas suficientes de protección; la publicidad comportamental dirigida a menores; la reincidencia en infracciones graves; la negativa injustificada a cumplir órdenes de la autoridad de aplicación; la falta de implementación del sistema de verificación exigido por la presente ley; la ausencia de medidas eficaces para prevenir, detectar o interrumpir situaciones de grooming; o deficiencias estructurales en sistemas de moderación, reporte, bloqueo o asistencia que permitan la reiteración de conductas vinculadas al abuso, explotación o captación de personas menores de edad. Serán sancionadas con multa de entre el tres por ciento (3%) y el cuatro por ciento (4%) de la facturación global anual, pudiendo disponerse la suspensión de actividades comerciales o publicitarias, la restricción severa de funcionalidades y planes obligatorios de adecuación.
- **Infracciones gravísimas:** incumplimientos sistemáticos, deliberados o persistentes que impliquen una grave afectación de los derechos de personas menores de edad, incluyendo: el incumplimiento sistemático y reiterado de las obligaciones establecidas en la presente ley; la negativa persistente a adecuarse al régimen legal; la exposición masiva de menores a riesgos graves; la obstaculización de auditorías o controles; la falta de cooperación con la autoridad de aplicación u otras autoridades competentes; permitir por acción u omisión, habiendo tenido conocimiento efectivo o debido conocer conforme a estándares razonables, la circulación, difusión o facilitación de material de abuso sexual infantil; o el incumplimiento de los deberes de remoción, bloqueo, denuncia de contenidos y cooperación frente a contenidos vinculados con grooming, abuso sexual infantil o explotación sexual infantil. Serán sancionadas con multa de entre el cuatro por ciento (4%) y el cinco por ciento (5%) de la facturación global anual, sin perjuicio de la aplicación de las medidas adicionales previstas en la presente ley.

Artículo 41°. Procedimiento y criterios de graduación. El procedimiento sancionatorio se regirá por la Ley N° 19.549 de Procedimientos Administrativos, su decreto reglamentario y normas concordantes, garantizando el debido proceso, el derecho de defensa, la producción de prueba, los mecanismos recursivos y el control judicial suficiente.

Para la graduación de las sanciones, la autoridad de aplicación deberá ponderar, especialmente:

- La gravedad de la infracción;
- La cantidad de personas menores de edad afectadas;
- El nivel de riesgo generado;
- El grado de intencionalidad o negligencia;
- El beneficio económico obtenido;
- La reincidencia;
- La capacidad económica del infractor;
- El grado de cooperación con la autoridad de aplicación;
- Las medidas de mitigación adoptadas;
- El historial de cumplimiento del proveedor.

La autoridad de aplicación podrá disponer medidas preventivas, correctivas o cautelares cuando existieren riesgos graves o inminentes para personas menores de edad, debiendo observar criterios de necesidad, proporcionalidad, razonabilidad y mínima afectación posible de los derechos de terceros.

Artículo 42°. Medidas excepcionales. El bloqueo de acceso al servicio en el territorio nacional solo podrá disponerse como medida excepcional y de *ultima ratio* frente a infracciones gravísimas, reiteradas y persistentes, previa:

1. Intimación fehaciente al proveedor;
2. Otorgamiento de un plazo razonable para su adecuación;
3. Sustanciación del procedimiento administrativo correspondiente;
4. Dictamen técnico-profesional fundado;
5. Garantía del derecho del proveedor a ser oído;
6. Intervención judicial previa y suficiente.

Las medidas adoptadas deberán limitarse estrictamente a lo necesario para la protección de los derechos de personas menores de edad, evitando afectaciones desproporcionadas sobre los derechos de terceros o sobre el acceso legítimo a la información y comunicación digital.

Artículo 43°. Interoperabilidad con el Sistema de Identidad Digital. Los proveedores deberán integrar sus sistemas con servicios estatales de validación de edad, tales como el Sistema de Identidad Digital (SID) del Registro Nacional de las Personas (RENAPER) o el que en el futuro lo reemplace, o con mecanismos equivalentes de consulta homologados por la autoridad de aplicación, que permitan consultas automatizadas, seguras, auditables y confidenciales, asegurando la privacidad.

La falta de integración efectiva, la utilización de mecanismos no homologados, la recolección excesiva de datos personales, la negativa injustificada de interoperar o el uso del sistema para finalidades distintas de las autorizadas constituirá una infracción gravísima según el régimen sancionatorio de la presente ley.

Artículo 44°. Plazo de adecuación de los proveedores. Los proveedores de servicios tendrán un plazo de ciento veinte (120) días corridos a partir de la publicación de la reglamentación de la presente ley para adecuar sus términos de servicio y sistemas tecnológicos de verificación.

La autoridad de aplicación podrá otorgar, por única vez y mediante resolución fundada, una prórroga de hasta sesenta (60) días corridos adicionales en caso de dificultades técnicas debidamente acreditadas.

Artículo 45°. Reverificación de cuentas. Las cuentas de usuarios menores existentes a la fecha de adecuación obligatoria de los proveedores deberán adecuarse a los parámetros establecidos en el artículo 15 de esta ley. En el caso de cuentas de menores de catorce (14) años de edad, estas se eliminarán o quedarán suspendidas hasta que el usuario alcance la edad habilitante.

Artículo 46°. Orden Público. Las disposiciones de la presente ley son de Orden Público.

Artículo 47°. Comuníquese al Poder Ejecutivo.

Diputado Nicolás Trotta.-

Diputada Roxana Monzón.-

Diputado Pablo Yedlin.-

Diputada María Jimena Lopez.-

Diputado Hugo Yasky.-

FUNDAMENTOS

Señor Presidente:

El presente proyecto se inscribe en una tendencia regulatoria global creciente que reconoce a los entornos digitales y, en particular, a las redes sociales, como espacios que generan riesgos específicos para niñas, niños y adolescentes, requiriendo por ello marcos normativos adecuados. En ese contexto, la reciente encíclica *Magnifica Humanitas* del Papa Francisco, del 15 de mayo de 2026 (publicada el 26 de mayo), es un llamado ético, filosófico y político a proteger la dignidad de las personas ante la transformación que la revolución digital ya impone en nuestra vida cotidiana. No resulta casual que su subtítulo sea "*sobre la custodia de la persona humana en los tiempos de la Inteligencia Artificial".* A los efectos de este documento, la tecnología no es neutra: "asume el rostro de quien la concibe, la financia, la regula y la utiliza". Por eso el llamado no es para rechazar la tecnología sino para regularla bajo criterios éticos sólidos.

La regulación es una responsabilidad compartida entre Estados, empresas, comunidades y familias, y sobre este principio se puede construir una comunidad justa, solidaria y humana. Nuestro país carece de una ley específica que regule el uso de sistemas digitales en relación con la protección de niñas, niños y adolescentes. Esta ausencia normativa genera un vacío de protección que contrasta con el intempestivo avance de las plataformas digitales, los sistemas de recomendación algorítmica y las herramientas de Inteligencia Artificial que los menores de edad utilizan cotidianamente en contextos educativos, de entretenimiento y de comunicación social. La encíclica *Magnifica Humanitas* ofrece un diagnóstico que resuena con la realidad argentina: la rapidez de la transformación tecnológica ha superado ampliamente la capacidad de respuesta del Estado. Las niñas, niños y adolescentes argentinos están expuestos a algoritmos diseñados para maximizar la atención y el compromiso, sin que existan salvaguardas suficientes para proteger su desarrollo cognitivo, emocional y social.

La idea de la presente norma es retrasar la edad en que nuestros niños, niñas y adolescentes se convierten en ciudadanos digitales en un entorno virtual. Lejos de constituir una iniciativa aislada, la regulación propuesta encuentra antecedentes en diversas jurisdicciones que han avanzado en la materia con distintos enfoques, pero con un diagnóstico común: la insuficiencia del paradigma de autorregulación de las plataformas y la necesidad de una intervención estatal activa.

En primer lugar, el caso de la Unión Europea plantea una regulación estructural basada en derechos digitales. La Unión Europea ha desarrollado uno de los marcos regulatorios más sofisticados en materia digital, centrado en la protección de derechos fundamentales. El Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos - RGPD) establece en su artículo 8° que el tratamiento de datos personales de menores en servicios de la sociedad de la información requiere el consentimiento parental cuando el usuario tenga menos de 16 años, habilitando a los Estados miembros a reducir ese umbral hasta los 13 años. Por su parte, el Reglamento (UE) 2022/2065 (Digital Services Act - DSA) introduce obligaciones específicas para plataformas digitales, en particular aquellas de gran escala, incluyendo: la evaluación y mitigación de riesgos sistémicos que afecten a menores (art. 34 y 35); la prohibición de publicidad dirigida basada en perfiles de menores (art. 28) y; la obligación de transparencia y auditabilidad de sistemas de recomendación (art. 27).

Asimismo, el Parlamento Europeo ha impulsado iniciativas orientadas a elevar la edad mínima de acceso a redes sociales y restringir prácticas de diseño adictivo. La regulación en este caso se estructura en torno a la protección de derechos fundamentales -privacidad, dignidad, desarrollo integral- y al control del tratamiento de datos personales como mecanismo central de tutela. Se trata de un modelo que prioriza la regulación estructural del ecosistema digital, evitando prohibiciones absolutas, pero imponiendo fuertes obligaciones a los proveedores.

En el caso de España se establece la consolidación de un enfoque de salud pública digital en línea con los desarrollos europeos. El Estado español ha avanzado en iniciativas legislativas orientadas a reforzar la protección de menores en entornos digitales. Recientemente, el Gobierno de España impulsó un proyecto para establecer la edad mínima de acceso a redes sociales en 16 años y la obligación de implementar sistemas efectivos de verificación de edad por parte de las plataformas. Estas medidas se inscriben en una estrategia más amplia de protección frente a los riesgos del entorno digital, incluyendo la exposición a contenidos nocivos, la desinformación y las dinámicas de uso compulsivo. En este caso, el enfoque se apoya en la consideración del uso intensivo de redes sociales como un problema de salud pública y bienestar juvenil, así como en la necesidad de corregir la falta de regulación efectiva del ecosistema digital. Se observa una transición desde el paradigma de la autorregulación hacia un esquema de responsabilidad empresarial reforzada.

También Australia estableció un modelo de prohibición y responsabilidad empresarial, el cual resulta el más restrictivo a nivel mundial hasta el momento. Mediante la *Online Safety Amendment (Social Media Minimum Age) Act 2024*, se estableció la prohibición de acceso a redes sociales para menores de 16 años, la obligación de las plataformas de impedir dicho acceso y un régimen sancionatorio severo, con multas de hasta 50 millones de dólares australianos. Esta normativa se encuentra vigente desde diciembre de 2025 y coloca la carga de cumplimiento exclusivamente sobre los proveedores, eximiendo de responsabilidad a padres y menores. Este enfoque australiano se basa en la evidencia sobre el impacto negativo de las redes sociales en la salud mental de adolescentes y en la constatación de que el diseño de estas plataformas responde a lógicas de captación de atención potencialmente adictivas. Se prioriza la prevención del daño mediante una prohibición clara, entendiendo que los mecanismos de control individual o familiar resultan insuficientes frente a riesgos sistémicos.

El caso de Brasil, en el ámbito regional, estableció una regulación del diseño y protección integral. Brasil ha sancionado la Ley N° 15.211/2025 (ECA Digital), que constituye uno de los antecedentes más relevantes para América Latina. Entre sus principales disposiciones se destacan: la vinculación obligatoria de cuentas de menores con sus progenitores o tutores; la prohibición de prácticas de diseño adictivo (scroll infinito, reproducción automática, notificaciones compulsivas); la prohibición de publicidad comportamental dirigida a menores; la imposición de obligaciones de transparencia y reportes periódicos y; un régimen sancionatorio basado en porcentajes de facturación. La ley presenta además alcance extraterritorial, aplicándose a cualquier servicio dirigido a usuarios en territorio brasileño. Se basa en la doctrina de la protección integral de la infancia, combinando regulación estatal, responsabilidad empresarial y participación de las familias. A diferencia del modelo australiano, no prohíbe el acceso en forma absoluta, sino que interviene sobre el diseño y funcionamiento de las plataformas, buscando reducir los riesgos estructurales.

Argentina carece hasta la fecha de un marco legal específico que regule este fenómeno con la integralidad que esto requiere. La brecha entre el avance tecnológico de las grandes plataformas y la capacidad regulatoria del Estado constituye, en los términos de la presente ley, una situación de riesgo institucional que el Poder Legislativo no puede pasar por alto y tiene el deber de corregir. La presente iniciativa responde a una urgencia que no admite más dilaciones: el creciente y documentado impacto del diseño adictivo de las plataformas digitales sobre la salud mental, el desarrollo biopsicosocial y la seguridad de niñas, niños y adolescentes.

El proyecto parte de una premisa jurídica y ética ineludible: las niñas, niños y adolescentes no pueden ser concebidos como meros usuarios o consumidores de tecnología, sino como personas titulares de derechos fundamentales, cuyo interés superior debe constituir una consideración primordial también en el diseño, funcionamiento y regulación de las plataformas digitales.

La Constitución de la Nación Argentina, en su artículo 75 inciso 22, otorga jerarquía constitucional a la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de Naciones Unidas el 20 de noviembre de 1989 y ratificada por la Argentina mediante la Ley N° 23.849. La

convención establece en su artículo 3° que el "interés superior del niño" debe ser una consideración primordial en todas las medidas que adopten las instituciones públicas o privadas que afecten a los niños. Por otro lado, el artículo 19 obliga a los Estados Partes a adoptar medidas legislativas, administrativas y sociales para proteger a los niños de toda forma de perjuicio o abuso. Asimismo, el Comité de los Derechos del Niño de Naciones Unidas ha emitido la Observación General N° 25, en el año 2021, relativa a los derechos del niño en relación con el entorno digital, en la que exhorta a los Estados a adoptar legislación específica para garantizar que el entorno digital sea seguro para los menores de edad, regular el diseño adictivo de las plataformas y exigir que las empresas de tecnología realicen evaluaciones de impacto sobre los derechos del niño.

En cuanto al marco regulatorio nacional, el artículo 19 de la Constitución Nacional garantiza el principio de autonomía personal, pero nuestra Carta Magna, siguiendo al propio texto de la Convención sobre los Derechos del Niño en su artículo 5°, reconoce que dicha autonomía es "progresiva" en el caso de los niños y los adolescentes: se adquiere gradualmente en función de la edad y la madurez. También la Ley N° 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes, sancionada el 28 de septiembre de 2005, establece en su artículo 3° el carácter de principio rector del interés superior del niño y en su artículo 9° el derecho a la dignidad e integridad personal. Esta norma fundamental define un sistema de responsabilidad concurrente entre el Estado, la familia y la sociedad en la protección de los menores, que el presente proyecto de ley en su artículo 34 extiende al dominio digital. En igual sentido, corresponde destacar que el presente proyecto se articula con el régimen de protección de datos personales vigente en la República Argentina, en particular con la Ley N° 25.326, que reconoce el derecho de toda persona al control de su información personal y establece principios de finalidad, proporcionalidad, calidad y seguridad en el tratamiento de datos. Estos principios resultan especialmente relevantes cuando se trata de personas menores de edad, cuya información requiere una protección reforzada, tal como ha sido sostenido por la Agencia de Acceso a la Información Pública en su carácter de autoridad de aplicación, la cual ha enfatizado la necesidad de adoptar medidas específicas de protección en entornos digitales, incluyendo mecanismos de verificación de edad, consentimiento informado y diseño de interfaces adaptadas al nivel de comprensión de los usuarios menores.

Por último, el Código Civil y Comercial de la Nación (Ley N° 26.994), en su artículo 1757, consagra la responsabilidad objetiva por actividades riesgosas o peligrosas para terceros. En este sentido, las plataformas digitales que emplean algoritmos de diseño adictivo dirigidos a menores de edad constituyen, en los términos de la norma, una actividad riesgosa cuyos generadores deben responder por los daños previsibles que ocasionen, salvo que acrediten haber adoptado todas las medidas razonables de prevención.

La "Ley de Cuidado y Bienestar Digital. Uso Responsable de Dispositivos y Redes Sociales para Niñas, Niños y Adolescentes" se inscribe en una tendencia global de marcos normativos destinados a proteger a las infancias en entornos digitales; por ello, los principios y artículos iniciales del proyecto (interés superior del menor, autonomía progresiva, diseño seguro por defecto, minimización de datos y protección frente a la hipervulnerabilidad) armonizan con estándares internacionales -como la Convención sobre los Derechos del Niño, las directrices de la UE sobre protección infantil en línea y las recomendaciones de la OCDE-, adaptando esas especificaciones a la realidad normativa y social argentina para garantizar la prevención del daño, la promoción de derechos digitales efectivos y la responsabilidad de proveedores y del Estado en todo el territorio nacional.

El artículo 1 establece el propósito central de la ley, que es asegurar que los menores de edad puedan ejercer plenamente sus derechos en el mundo digital, respetando su madurez y crecimiento (autonomía progresiva) y priorizando siempre su bienestar, en sintonía con nuestra normativa vigente. El artículo 2 define el marco normativo de la ley, que consiste en establecer un marco regulatorio para el uso responsable de las redes sociales y servicios análogos en el territorio nacional, priorizando la protección de las infancias, las adolescencias y las familias y la creación de

entornos digitales que prevengan y minimicen de manera eficaz el daño. Continuando con esta línea, el artículo 3 fija los pilares conceptuales que guiarán la aplicación de la norma, tales como el interés superior del menor, la autonomía progresiva, el diseño seguro por defecto, la minimización de la recopilación de datos y la protección específica ante la hipervulnerabilidad digital.

El artículo 4 atribuye una responsabilidad subjetiva agravada y directa a las empresas proveedoras de redes sociales quedando comprendidas la modalidad técnica, soporte, modelo de negocio o tecnología utilizada, las redes sociales, servicios de mensajería individual o grupal y plataformas de intercambio de contenidos que asumen la obligación ineludible de prevención, mitigación y reparación de daños, sin poder eximirse invocando conductas de terceros o la mera responsabilidad parental. El artículo 5 prohíbe el diseño e implementación de sistemas automatizados de recomendación y mecanismos de perfilamiento que utilicen datos de menores de 18 años con el fin de retener compulsivamente su atención o manipular sus hábitos de consumo. En la misma línea, el artículo 6 establece un régimen escalonado frente a las agresivas estrategias del marketing digital. Hoy en día, las plataformas de internet usan algoritmos avanzados para rastrear lo que hacen los chicos, conocer sus gustos y mostrarles anuncios personalizados difíciles de esquivar. Esto genera una manipulación comercial que los menores no siempre pueden detectar. Con el finde solucionar esto, el articulo propone una protección máxima para menores de 16 años y una protección intermedia para jóvenes de 16 y 17 años. Por otro lado, el artículo 7, prohíbe por completo en toda la Argentina promocionar, publicitar o patrocinar casinos online y apuestas en línea en cualquier aplicación, red social o plataforma digital.

Asimismo se delimita el alcance de la ley en el artículo 8, determinando que quedan sujetos a ella todos los proveedores que ofrezcan servicios directos o indirectos en la República Argentina o cuyos efectos impacten en el territorio nacional, independientemente de dónde se encuentren físicamente sus servidores (excluyendo a las plataformas con fines meramente educativos, sanitarios o laborales). Como refuerzo de esto, el artículo 9 obliga a los proveedores extranjeros a constituir una sucursal local, registrar un domicilio legal ante la autoridad de aplicación y designar representantes legales con domicilio en el país y facultades suficientes para responder penal, civil y administrativamente, bajo apercibimiento de bloqueo del servicio ante su incumplimiento.

El artículo 10 declara que proteger el bienestar mental y la privacidad de los menores en internet es una prioridad nacional buscando cuidar la capacidad de atención de los jóvenes, que decidan por sí mismos cuánto tiempo usan los dispositivos sin manipulación y evitar que el uso intensivo dañe su descanso o su educación. Asimismo, prescribe en el artículo 11 que los contenidos sobre salud o medicina de ejercicio regulado solo se muestren si provienen de perfiles con matrícula profesional verificada y vigente.

Con el artículo 12, el proyecto propone maximizar el tiempo fuera de las interfaces virtuales restringiendo el uso de los teléfonos celulares y dispositivos digitales personales durante las horas de clase en los tres niveles de la educación obligatoria nacional. Esta prohibición alcanza tanto a alumnos como a docentes, contemplando excepcionalidades únicamente guiadas con fines estrictamente pedagógicos o por razones de discapacidad y accesibilidad. Cada provincia controlará que esto se cumpla.

En los siguientes artículos, tipifica y conceptualiza las características estructurales que transforman a una plataforma en un ambiente de riesgo, describiendo en el artículo 13 el diseño conductual dependiente, los algoritmos opacos de recomendación, la interacción social irrestricta con desconocidos y la exposición a contenidos problemáticos, incluyendo aquellos que promuevan la violencia, conductas peligrosas, autolesiones, suicidio o resulten incompatibles con la protección integral del menor. El artículo 14 clasifica técnicamente los entornos digitales en tres escalas: riesgo leve, moderado o alto/crítico, atendiendo a la intensidad de sus funciones, su potencial capacidad de daño y la suficiencia de sus herramientas de mitigación.

El Capítulo II establece las condiciones de acceso, el entorno digital saludable y la prevención de daños para garantizar el buen uso. En primer lugar, el artículo 15 segmenta el acceso por edades, prohibiendo el uso de redes sociales a menores de catorce (14) años; fija un acceso restringido para niñas, niños y adolescentes de entre catorce (14) y dieciséis (16) años previa autorización parental; y establece un acceso condicionado a partir de los dieciséis (16) años de edad cumplidos, pero bajo configuraciones protectoras automáticas y derecho de oposición parental hasta la mayoría de edad. El artículo 16, por otro lado, impone a las empresas el deber de proveer de forma nativa o integrada recursos técnicos de control parental y emparejamiento familiar (reportes mensuales, límites de tiempo en dispositivos y filtros de descargas) respetando el desarrollo autónomo del menor de edad.

En el artículo 17 el proyecto asegura el derecho fundamental de las niñas, niños y adolescentes a recibir información adecuada, completa y veraz; a contar con instancias de revisión ante decisiones automatizadas de las plataformas; y a disponer de mecanismos ágiles para impugnar bloqueos de cuenta erróneos. En cuanto al sistema de verificación de edad, estipulado en el artículo 18, obliga a los proveedores a contar con sistemas de verificación técnica de la edad, excluyendo la mera autodeclaración como único filtro. También garantiza que los datos no sean almacenados más allá del tiempo necesario para completar el proceso y que cuenten con controles de reverificación de edad cada 12 meses. El incumplimiento de esto será considerado una infracción grave a los efectos sancionatorios de esta ley.

El artículo 19 protege la privacidad de menores y previene el uso indebido de sus datos personales, garantizando que la recopilación etaria no vulnere derechos fundamentales ni se convierta en un mecanismo de explotación comercial. Seguidamente, el artículo 20, con el Protocolo de "Prueba de Edad", refuerza la protección de datos personales con un sistema seguro, evitando la exposición innecesaria de información sensible, conforme a principios internacionales de protección de datos y privacidad. El artículo 21 establece los parámetros para usuarios extranjeros que no posean Documento Nacional de Identidad o ante fallas sistémicas, evitando la discriminación por nacionalidad o por fallos técnicos.

Una de las principales garantías para las cuentas de niñas, niños y adolescentes es la configuración de privacidad protectora por defecto, estipulada en el artículo 22. En ella se establece que todas las cuentas de usuarios menores de edad deben activar el máximo nivel de privacidad, como por ejemplo la desactivación de geolocalización en tiempo real, la restricción de publicaciones solo a contactos aprobados y la inhabilitación para indexación en buscadores de manera que se minimicen los riesgos de vulnerabilidad en los entornos digitales. En el artículo 23 se establece que las aplicaciones y redes sociales deben cerrar por defecto el chat privado de los menores. Solo podrán recibir mensajes de personas que ya tengan en su lista de contactos. Si un adulto quiere escribirles, no bastará con que el menor lo acepte: la plataforma exigirá obligatoriamente que ese adulto tenga su identidad validada y cuenta verificada de forma fehaciente.

El artículo 24 explicita que facilitar la comprensión de la información contractual asegura que el usuario menor de edad pueda ejercer sus derechos con pleno conocimiento, fomentando un entorno digital seguro y responsable. A continuación se define el marco de reglamentación para la Inteligencia Artificial. En el artículo 25 fija que cuando un usuario menor de edad utilice estas herramientas, las empresas dueñas de esa tecnología serán responsables legales directas de que el sistema respete su salud mental, su desarrollo integral y su autonomía progresiva. Las mismas deben establecer filtros de seguridad y bloqueo de contenidos dañinos; cuando un usuario menor de edad busca o pregunta sobre suicidio, trastornos alimentarios, apuestas online, pornografía, violencia o ciberacoso, el sistema tiene prohibido responder o generar textos o imágenes sobre eso (artículo 26). Por último, con respecto a este tema, el artículo 27 define un Protocolo Automático de Gestión, Alerta y Derivación Asistida ante Crisis, el cual debe bloquear el contenido frente a una detección de crisis, posteriormente debe informar sobre teléfonos de ayuda gratuita y mandar una alerta confidencial a las cuentas de los padres que estén vinculadas a la supervisión familiar.

En el artículo 28, las plataformas deben medir el tiempo que los usuarios menores de edad pasan conectados. En el caso de detectar un uso excesivo, tienen que lanzar alertas que sugieran tomarse un descanso y, con el objetivo de frenar la adicción, se prohíbe usar la reproducción automática infinita y los sistemas de premios por quedarse conectados. Además, no podrán usar estos datos de consumo para venderles publicidad.

El artículo 29 pone la lupa en el mundo del gaming. Cualquier videojuego o plataforma multijugador que usen menores de 18 años queda obligado por ley a diseñar sus entornos cuidando la salud emocional de los jugadores y previniendo conductas adictivas. El artículo 30 prohíbe explícitamente los trucos de diseño que usan los videojuegos para enganchar a los chicos. Quedan vedados los premios variables que manipulan la conducta, los algoritmos que buscan debilidades emocionales para vender más y las mecánicas de apuestas disfrazadas. Tampoco pueden recomendar contenido violento o adulto.

También, en el artículo 31, se trata de delimitar la inclusión financiera de los jóvenes para dotarlo de un entorno seguro. Las neurociencias y la psicología advierten que los sistemas de recompensa de los adolescentes son altamente vulnerables a los estímulos de las apuestas en línea. Al exigir que las billeteras virtuales actúen como un filtro activo, el Estado delega la responsabilidad tecnológica en quienes controlan las pasarelas de pago, protegiendo de forma efectiva el patrimonio familiar y la salud mental de los menores. En el artículo 32, las empresas de internet tienen que mantener activos sistemas de detección temprana para frenar a tiempo problemas graves como el grooming, la ludopatía digital, la anorexia, la explotación sexual infantil o la depresión. Si saltan las alarmas, deben frenar la difusión de ese contenido riesgoso, ofrecer ayuda inmediata en los dispositivos y avisar a los adultos responsables.

Por último, el artículo 33 propone la verificación de edad para páginas pornográficas. Cualquier plataforma que aloje o comercialice pornografía deberá poner una barrera previa y efectiva de verificación de edad para que el sistema bloquee de forma absoluta el ingreso de menores de edad, bajo penas de sanciones gravísimas.

El Capítulo III establece en el artículo 34 que la Agencia de Acceso a la Información Pública (AAIP) será la autoridad de aplicación trabajando en coordinación con la Defensoría de los Derechos de las Niñas, Niños y Adolescentes. Entre sus funciones principales tendrá que controlar el cumplimiento de la ley, recibir denuncias, aplicar sanciones, realizar auditorías y estudios de impacto y publicar un Informe Anual para remitir al Congreso.

El Estado debe comprometerse a garantizar educación digital, capacitación docente, programas de prevención de salud mental, canales de denuncia y apoyo familiar, según el artículo 35, focalizado en la responsabilidad concurrente que posee. Aquí, como punto fundamental, se establece que la responsabilidad de los padres no exime ni reduce las obligaciones legales del Estado ni de los proveedores de medios digitales. Para aportar certeza en el manejo, el artículo 36 obliga a las empresas a presentar un Informe Público de Transparencia cada seis meses ante este Honorable Congreso Nacional y la Agencia de Acceso a la Información Pública (AAIP). El documento deberá incluir estadísticas detalladas de usuarios menores de edad, contenidos eliminados o cuentas bloqueadas, medidas de control parental aplicadas, auditorías de efectividad y propuestas de mejora. Estos informes se debatirán en una posible convocatoria de audiencia pública anual.

El Fondo de Promoción de la Salud Digital (FPSD) que crea el artículo 37 se financiará con las multas cobradas y una nueva Tasa de Prevención Digital (artículo 38). El dinero será exclusivamente utilizado para financiar herramientas de bienestar digital mediante la prevención, las campañas de concientización, investigaciones, etc., con el fin de generar un ámbito de entornos digitales saludables para los menores de edad. Por su parte, la tasa previamente mencionada es una contribución anual obligatoria para disminuir el impacto negativo de los algoritmos y los modelos de negocios que involucren a usuarios menores de edad.

Por último, el Capítulo IV establece el Régimen de Responsabilidad, las Sanciones y las Disposiciones complementarias. El artículo 39 define las herramientas de sanción que tiene la autoridad de aplicación frente a los incumplimientos de las empresas. Se enmarcan desde un apercibimiento hasta multas sobre su facturación global (artículo 40) de acuerdo con la consideración de la falta cometida. También considera la suspensión de publicidad, la baja de ciertas funciones que provean e incluso el bloqueo total del servicio en el país como medida extremísima. En concordancia con todo esto, el artículo 41 establece que las sanciones deben respetar la Ley de Procedimientos Administrativos (N° 19.549) y que, para fijar el monto de las multas, la Agencia de Acceso a la Información Pública (AAIP) deberá poner el foco en cuántos usuarios menores fueron afectados, la intencionalidad, el tamaño de la empresa y su nivel de cooperación frente a la resolución del problema. También permite dictar medidas cautelares urgentes para proteger a los usuarios menores de edad.

Como medida extrema y excepcional, en el artículo 42 se puede realizar el bloqueo de una plataforma como recurso de última instancia ante faltas gravísimas y repetitivas mediante un proceso estricto que debe seguir la siguiente línea: intimación previa, plazo de adecuación, dictámenes técnicos, el derecho a réplica y, fundamentalmente, la autorización de un juez.

Frente a la necesidad de verificación de identidad, el proyecto exige a las empresas conectar sus sistemas con herramientas estatales de validación de identidad, tales como el Sistema de Identidad Digital (SID) del Registro Nacional de las Personas (RENAPER), garantizando en el artículo 43 que el proceso sea automatizado, seguro y que cuide la privacidad de los datos personales. Como últimas medidas, la iniciativa le otorga a las plataformas un tiempo de 120 días corridos para actualizar sus contratos, términos de servicios y sistemas de control de edad a partir de la reglamentación de la ley (artículo 44) y obliga a la reverificación de las cuentas de usuarios menores de edad que ya existen para cumplir con lo estipulado según las edades de acceso de la presente ley (artículo 45). Finalmente, el artículo 46 declara que esta legislación es de Orden Público, lo que significa que sus normas son de cumplimiento obligatorio dentro del territorio argentino.

Por todo lo anteriormente mencionado, Señor Presidente, la evidencia y los marcos internacionales también muestran que los riesgos que enfrentan niñas, niños y adolescentes en el entorno digital no son conjeturales ni marginales. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha advertido que los niños enfrentan en línea riesgos graves, entre ellos explotación y abuse, violaciones a la privacidad, diseño manipulativo y algoritmos que amplifican daños, y ha señalado de manera explícita que ciertas formas de perjuicio, como la explotación y el abuso sexual infantil, los afectan de manera específica. La OCDE, por su parte, ha destacado que el entorno digital es hoy una parte integral de la vida cotidiana de los niños y que los riesgos han cambiado de escala y naturaleza, al punto de requerir nuevas respuestas regulatorias. UNICEF ha señalado asimismo la urgencia de fortalecer las respuestas frente a la explotación y el abuso sexual infantil en línea. En ese marco, no se puede aceptar una mirada neutral o ingenua sobre el funcionamiento de plataformas cuya arquitectura puede facilitar el contacto inapropiado, la captación de menores, la exposición a contenidos dañinos o la prolongación compulsiva de la permanencia.

En este sentido, resulta imprescindible reconocer que las plataformas digitales no constituyen meros espacios neutrales de interacción, sino que se han convertido en verdaderos canales de comunicación estructurales que, en muchos casos, permiten, facilitan o amplifican la vulneración de derechos de niñas, niños y adolescentes. La arquitectura misma de estas plataformas - basada en la interacción abierta, el anonimato relativo, la viralización de contenidos y la intermediación algorítmica- ha generado condiciones que posibilitan fenómenos tales como el acoso, la captación con fines de abuso, la exposición a contenidos inapropiados y la manipulación psicológica. En particular, en materia de abuso y explotación sexual infantil, las redes sociales han sido identificadas como uno de los principales medios de contacto, aproximación y consolidación del vínculo entre agresores y víctimas.

No se trata, por tanto, de riesgos abstractos o meramente potenciales, sino de situaciones concretas y verificables en las que el entorno digital funciona como vehículo necesario para la comisión de determinadas conductas lesivas. En este contexto, sostener que las plataformas son simples intermediarias pasivas implica desconocer su rol estructural en la configuración del espacio donde estos hechos tienen lugar. Por el contrario, corresponde reconocer que, en la medida en que organizan, diseñan y administran estos entornos de interacción, también tienen la capacidad -y, por ende, la responsabilidad-de prevenir, mitigar y reducir los riesgos previsibles asociados a su funcionamiento.

Desde esta perspectiva, el presente proyecto no parte de una lógica sancionatoria aislada, sino de una comprensión integral del ecosistema digital, en la cual las plataformas son entendidas como actores centrales en la dinámica de producción de riesgos. En consecuencia, la regulación propuesta busca intervenir no solo sobre las conductas individuales, sino también sobre las condiciones estructurales que hacen posible la vulneración de derechos, estableciendo obligaciones concretas de diseño seguro, verificación de identidad y debida diligencia digital.

Claramente, la relación entre usuarios, especialmente menores de edad, y plataformas digitales se encuentra atravesada por una profunda asimetría de información, capacidad técnica y poder económico. Las grandes plataformas tecnológicas cuentan con equipos especializados en neurociencia, diseño conductual y análisis masivo de datos orientados a optimizar la captación de la atención. En contraposición a esto, las familias y los propios menores de edad carecen de esas herramientas equivalentes para comprender y mitigar estos efectos. Por ello, la intervención estatal no constituye una restricción indebida de las libertades individuales, sino una condición necesaria para garantizar un entorno digital equitativo, seguro y compatible con los derechos humanos.

La necesidad de legislar específicamente sobre el acceso de personas menores de edad a plataformas de redes sociales se vuelve todavía más evidente a la luz de los estándares internacionales más recientes. La Observación General Nº 25 del Comité de los Derechos del Niño, dedicada precisamente a los derechos de niñas, niños y adolescentes en relación con el entorno digital, constituye un hito normativo de primer orden porque afirma de manera expresa que los derechos de la niñez rigen tanto en el ámbito offline como online, y exige a los Estados adoptar medidas legislativas, administrativas y de otra índole para protegerlos en el mundo digital. No se trata, entonces, de forzar artificialmente categorías tradicionales sobre una realidad tecnológica novedosa, sino de cumplir con una interpretación autorizada y contemporánea de obligaciones internacionales ya vigentes para la República Argentina. La discusión internacional ya no gira en torno a si corresponde intervenir, sino en cómo hacerlo de manera eficaz y respetuosa de los derechos fundamentales.

Por último, la implementación de esta ley requerirá la articulación entre el Estado Nacional, las provincias y la Ciudad Autónoma de Buenos Aires, dándole un enfoque federal que permitirá adaptar las políticas de prevención, educación digital y asistencia a las realidades territoriales, fortaleciendo la eficacia de la norma.

Es por todo esto, Señor Presidente, que tengo la convicción de que estamos definiendo las condiciones en las que una generación entera va a desarrollarse, vincularse y construir su identidad. La encíclica *Magnifica Humanitas* del Papa Francisco ofrece un horizonte ético y filosófico de primer orden para fundamentar la intervención legislativa en materia de protección de las niñas, niños y adolescentes frente a los entornos digitales en los cuales están inmersos. Su llamado a "custodiar lo humano en la transformación" y a proteger especialmente a los más frágiles tiene una traducción normativa clara: los Estados deben actuar con urgencia para establecer marcos regulatorios que los pongan por sobre los intereses comerciales del sector tecnológico; no se puede permanecer neutral frente a modelos de negocios que obtienen rentabilidad a partir de la captación intensiva de los usuarios menores de edad.

Este proyecto no prohíbe, no censura ni limita la innovación. Por el contrario, establece reglas claras para que el desarrollo tecnológico sea compatible con los derechos humanos. Es una medida para retrasar la edad en que los jóvenes se convierten en ciudadanos de un esquema de redes sociales. Regular hoy es cuidar el presente y garantizar el futuro. Argentina tiene una enorme oportunidad de inscribirse en la vanguardia de una regulación que no frena la innovación, sino que la orienta hacia el bien común. Debemos consensuar una legislación que tome en serio el desafío y que haga del cuidado de las infancias un principio rector irrenunciable.

Este proyecto trata de fijar las bases para edificar una sociedad más justa, más humana y más digna. Por las razones expuestas, solicito a mis pares el acompañamiento en la presente iniciativa legislativa.

Diputado Nicolás Trotta.-

Diputada Roxana Monzón.-

Diputado Pablo Yedlin.-

Diputada María Jimena Lopez.-

Diputado Hugo Yasky.-