DIPUTADOS
ARGENTINA

PROYECTO DE LEY

EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA
REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY:

LEY DE VERIFICACIÓN DE EDAD Y PROTECCIÓN DE MENORES EN ENTORNOS DIGITALES

Sistema Integral de Verificación de Edad para Menores en Entornos Digitales (SIVEM)

TÍTULO I — DISPOSICIONES GENERALES

ARTÍCULO 1°. ***Objeto.*** La presente ley tiene por objeto establecer el Sistema Integral de Verificación de Edad para Menores en Entornos Digitales (SIVEM), destinado a: a) Proteger a niños, niñas y adolescentes frente a los riesgos derivados del uso de plataformas digitales y redes sociales; b) Garantizar mecanismos de verificación de edad eficaces, respetuosos de la privacidad, técnicamente viables y soberanamente gestionados; c) Establecer obligaciones diferenciadas para las plataformas digitales según su escala y riesgo sistémico; d) Preservar el derecho de los menores al acceso a la información, la educación, la salud y la expresión en entornos digitales seguros; e) Proteger la responsabilidad parental y el rol de los padres, madres y tutores legales; f) Garantizar los derechos procesales del menor en el entorno digital.

ARTÍCULO 2°. ***Ámbito de aplicación.*** La presente ley se aplica a toda plataforma digital que opere o sea accesible desde el territorio de la República Argentina y que permita la interacción social entre usuarios, la publicación de contenido generado por usuarios, o el consumo de contenido personalizado mediante algoritmos de recomendación, así como a los proveedores de servicios de verificación de edad que operen en relación con dichas plataformas.

ARTÍCULO 3°. ***Definiciones.*** A los efectos de la presente ley, se entiende por: a) Menor: toda persona menor de dieciocho (18) años de edad conforme la legislación argentina; b) Plataforma digital regulada: todo servicio de la sociedad de la información cuyo propósito principal o significativo sea permitir la interacción social entre usuarios, incluyendo pero no limitado a redes sociales, plataformas de video de contenido generado por usuarios, servicios de streaming con funcionalidades sociales y foros de interacción pública; c) Plataforma de muy gran escala (PMGE): toda plataforma digital regulada que cuente con más de cuatro millones (4.000.000) de usuarios activos mensuales en la República Argentina o que, por la naturaleza de sus funcionalidades, represente un riesgo sistémico significativo para menores conforme los criterios del artículo 25; d) Funcionalidades adictivas: características de diseño deliberadamente orientadas a maximizar el tiempo de permanencia del usuario mediante mecanismos de refuerzo variable, incluyendo scroll infinito, reproducción automática, notificaciones de activación conductual, métricas de validación social y sistemas de recompensa intermitente; e) Token de edad: credencial digital criptográfica emitida por un emisor certificado dentro del SINAVE que certifica que su titular se encuentra dentro de un rango etario determinado, sin revelar identidad, fecha de nacimiento exacta ni ningún otro dato personal; f) Prueba de conocimiento cero: protocolo criptográfico que permite demostrar la veracidad de una afirmación sin revelar información adicional; g) Verificación de edad: proceso por el cual se determina de manera fehaciente si un usuario supera un umbral de edad determinado; h) Estimación de edad: proceso por el cual se estima de manera probabilística la edad de un usuario mediante análisis biométrico; i) Consentimiento parental verificable: autorización otorgada por el padre, madre o tutor legal del menor, cuya identidad y relación parental han sido verificadas por medios fehacientes; j) Deber de diligencia reforzada: obligación general de las plataformas de diseñar, desarrollar y operar sus servicios priorizando la seguridad y el bienestar de los menores; k) Riesgo sistémico: riesgo significativo de daño a la salud mental, la seguridad, la privacidad o los derechos fundamentales de menores, derivado de la escala, el diseño o el funcionamiento de una plataforma; l) Autoridad de Aplicación: la Agencia Nacional de Protección Digital de Menores creada por el artículo 49 de la presente ley; m) RENAPER: Registro Nacional de las Personas; n) SINAVE: Sistema Nacional de Verificación de Edad creado por el artículo 10 de la presente ley.

ARTÍCULO 4°. ***Principios rectores.*** La implementación de la presente ley se rige por los

siguientes principios: a) Interés superior del niño, conforme la Convención sobre los Derechos del Niño y la Ley 26.061; b) Proporcionalidad, conforme el artículo 5 de la presente ley; c) Minimización de datos: solo se procesa la información estrictamente necesaria para la verificación de edad; d) Soberanía digital: la infraestructura de verificación de edad es gestionada conforme una arquitectura federada con el Estado argentino como raíz de confianza; e) Privacidad por diseño: los sistemas de verificación se diseñan para proteger la privacidad desde su concepción; f) No discriminación: los sistemas de verificación no deben excluir ni perjudicar a personas por razón de su origen, etnia, condición socioeconómica, discapacidad o cualquier otra condición; g) Responsabilidad de las plataformas: la carga de implementar y cumplir la verificación recae sobre las plataformas, no sobre los menores ni sus familias; h) Transparencia algorítmica; i) Interoperabilidad; j) Regulación basada en riesgo: las obligaciones son proporcionales al riesgo sistémico de cada plataforma; k) Regulación basada en resultados: la eficacia de las medidas se mide mediante indicadores verificables.

ARTÍCULO 5°. ***Test de proporcionalidad.*** Toda medida técnica, administrativa o regulatoria adoptada en el marco de la presente ley deberá superar un test de proporcionalidad en tres niveles: a) Idoneidad: la medida debe ser apta para alcanzar el objetivo legítimo de protección del menor; b) Necesidad: no debe existir una medida alternativa igualmente eficaz que resulte menos restrictiva de los derechos del menor, de los usuarios adultos o de la libertad de empresa; c) Proporcionalidad estricta: los beneficios de la medida para la protección de menores deben ser superiores a las restricciones que impone sobre otros derechos e intereses. La Autoridad de Aplicación debe documentar el cumplimiento de este test para cada estándar técnico, resolución sancionatoria o medida de ejecución que adopte. Las plataformas digitales reguladas pueden invocar el incumplimiento de este test como fundamento de impugnación administrativa o judicial de cualquier acto de la Autoridad de Aplicación.

TÍTULO II — RÉGIMEN DE EDAD Y ACCESO ESCALONADO

ARTÍCULO 6°. ***Prohibición de acceso a menores de trece (13) años.*** Las plataformas digitales reguladas tienen prohibido permitir la creación o mantenimiento de cuentas por parte de personas menores de trece (13) años. Esta prohibición no admite excepción por consentimiento parental, salvo para plataformas exclusivamente educativas

certificadas por el Ministerio de Educación o de salud certificadas por el Ministerio de Salud, conforme el artículo 9.

ARTÍCULO 7°. ***Acceso con consentimiento parental verificable para menores de trece (13) a quince (15) años.*** Las personas de trece (13) a quince (15) años podrán acceder a plataformas digitales reguladas exclusivamente con consentimiento parental verificable, otorgado conforme los mecanismos establecidos en el Título III. El acceso se realiza en modalidad protegida conforme el artículo 8.

ARTÍCULO 8°. ***Modalidad protegida.*** La modalidad protegida implica que la plataforma digital regulada debe, como mínimo: a) Desactivar por defecto todas las funcionalidades adictivas definidas en el artículo 3 inciso d); b) Desactivar por defecto la recepción de notificaciones entre las veintidós horas (22:00) y las siete horas (7:00), salvo configuración parental en contrario; c) Limitar por defecto la visibilidad del perfil del menor a sus contactos aprobados; d) Desactivar por defecto el contacto por mensajería directa de cuentas no seguidas por el menor; e) Impedir la publicidad dirigida basada en perfilamiento conductual o psicográfico del menor; f) Excluir al menor de los sistemas de recomendación algorítmica personalizada, ofreciendo contenido curado por orden cronológico o categorial; g) Implementar un panel parental que permita monitorear tiempo de uso y categorías de contenido, sin acceso al contenido de mensajes privados; h) Ofrecer herramientas accesibles de denuncia con respuesta dentro de los plazos que establezca la reglamentación. Las personas de dieciséis (16) a diecisiete (17) años podrán acceder a plataformas digitales reguladas sin consentimiento parental, previa verificación de edad conforme el Título III. El acceso se realiza en modalidad protegida, salvo que el menor opte expresamente por la modalidad estándar con notificación al titular de la responsabilidad parental. La reglamentación podrá ampliar las condiciones de la modalidad protegida conforme la evolución tecnológica y la evidencia científica.

ARTÍCULO 9°. ***Exclusiones.*** La presente ley no se aplica a: a) Servicios de mensajería interpersonal sin funcionalidades de publicación abierta, perfiles públicos ni algoritmos de recomendación; b) Plataformas de videojuegos sin funcionalidades sociales equivalentes a una red social; c) Plataformas educativas certificadas por el Ministerio de Educación; d) Plataformas de salud y bienestar certificadas por el Ministerio de Salud; e) Enciclopedias colaborativas, bibliotecas digitales y repositorios de conocimiento abierto; f) Servicios de correo electrónico.

TÍTULO III — SISTEMA NACIONAL DE VERIFICACIÓN DE EDAD (SINAVE)

ARTÍCULO 10°. ***Creación.*** Créase el Sistema Nacional de Verificación de Edad (SINAVE), como infraestructura soberana de verificación de edad para entornos digitales, administrado por la Autoridad de Aplicación en coordinación con el RENAPER.

ARTÍCULO 11°. ***Arquitectura federada.*** El SINAVE opera bajo una arquitectura federada de emisores de tokens de edad, conforme las siguientes reglas: a) El Estado argentino, a través del RENAPER, actúa como raíz de confianza del sistema; b) Pueden actuar como emisores certificados de tokens de edad el RENAPER directamente, entidades públicas provinciales o municipales habilitadas por la Autoridad de Aplicación, y entidades privadas certificadas que cumplan los estándares técnicos, de seguridad y de privacidad establecidos por la Autoridad de Aplicación; c) Todos los emisores certificados operan bajo protocolos criptográficos interoperables y están sujetos a auditoría periódica; d) Ningún emisor certificado puede almacenar, retener ni procesar datos personales más allá de lo estrictamente necesario para la emisión del token; e) La Autoridad de Aplicación puede revocar la certificación de cualquier emisor que incumpla los estándares establecidos; f) La arquitectura federada se diseña para evitar puntos únicos de fallo, garantizando la continuidad del servicio ante la indisponibilidad de cualquier emisor individual. La reglamentación determinará los protocolos criptográficos específicos, los procedimientos de certificación de emisores, los estándares de seguridad y las condiciones de auditoría.

ARTÍCULO 12°. ***Funcionamiento.*** El SINAVE opera conforme el siguiente flujo: a) El usuario o su representante legal solicita un token de edad a través de cualquier emisor certificado; b) El emisor verifica la identidad y la edad del solicitante contra la base de datos del RENAPER mediante protocolos seguros; c) Verificada la edad, el emisor emite un token criptográfico que certifica exclusivamente que el titular se encuentra en un rango etario determinado conforme las franjas que establezca la reglamentación; d) El token no contiene ni permite inferir nombre, documento nacional de identidad, fecha de nacimiento exacta ni ningún otro dato personal; e) El token se almacena localmente en el dispositivo del usuario, cifrado y vinculado al dispositivo; f) Cuando una plataforma solicita verificación, el usuario presenta el token, que transmite exclusivamente una respuesta binaria sin revelar rango etario ni datos adicionales; g) La plataforma no puede almacenar, copiar ni retransmitir el token.

ARTÍCULO 13°. ***Verificación de consentimiento parental.*** Para menores de trece (13) a quince (15) años, el SINAVE implementa un flujo adicional de consentimiento parental verificable: a) El padre, madre o tutor solicita un token de consentimiento parental; b) El emisor verifica la identidad del adulto y la relación parental o tutolar contra las bases del RENAPER y del Registro Civil correspondiente; c) Se emite un token de consentimiento vinculado al token de edad del menor; d) El token de consentimiento es revocable en cualquier momento con efecto inmediato.

ARTÍCULO 14°. ***Gratuidad.*** La emisión de tokens de edad y de consentimiento parental por el RENAPER y por las entidades públicas emisoras es gratuita para los usuarios. Los emisores privados certificados pueden cobrar únicamente los costos operativos que autorice la Autoridad de Aplicación.

ARTÍCULO 15°. ***Estimación de edad como método subsidiario.*** Cuando el usuario no disponga de token vigente y la plataforma requiera verificación inmediata, se permite la estimación de edad por medios biométricos, sujeta a: a) Procesamiento exclusivamente local en el dispositivo del usuario; b) Eliminación inmediata de los datos biométricos después de la estimación; c) Resultado exclusivamente binario; d) Certificación del proveedor de tecnología por la Autoridad de Aplicación; e) Si la estimación es ambigua, el sistema debe requerir verificación mediante token. La estimación de edad no sustituye la obligación de integración con el SINAVE. La reglamentación establecerá los estándares de precisión, los requisitos de certificación de proveedores y los plazos máximos de retención.

ARTÍCULO 16°. ***Reverificación periódica.*** Las plataformas deben reverificar periódicamente las cuentas de menores y adultos, con frecuencias diferenciadas según el rango etario, mediante token actualizado o estimación subsidiaria. La reglamentación determinará las frecuencias mínimas de reverificación.

ARTÍCULO 17°. ***Interoperabilidad.*** El token de edad del SINAVE es interoperable entre todas las plataformas que operen en el territorio nacional. La Autoridad de Aplicación publica las especificaciones técnicas como estándar abierto y promueve su compatibilidad con marcos internacionales de identidad digital y credenciales verificables, incluyendo el marco eIDAS de la Unión Europea, los estándares W3C de credenciales verificables e identidad descentralizada, y los marcos de identidad digital del MERCOSUR. La Autoridad de Aplicación actualiza las especificaciones de

interoperabilidad periódicamente conforme determine la reglamentación.

ARTÍCULO 18°. ***Código abierto.*** El software del SINAVE se desarrolla y publica como código abierto, auditable por cualquier persona. Las bibliotecas criptográficas, protocolos de comunicación y documentación técnica son de acceso público.

TÍTULO IV — OBLIGACIONES DE LAS PLATAFORMAS DIGITALES

ARTÍCULO 19°. ***Deber de diligencia reforzada.*** Las plataformas digitales reguladas tienen un deber general de diligencia reforzada respecto del diseño, desarrollo, operación y actualización de sus servicios cuando estos sean utilizados o accesibles por menores. Este deber implica anticipar, prevenir y mitigar los riesgos razonablemente previsibles que el diseño de la plataforma pueda generar para la salud mental, la seguridad, la privacidad y los derechos fundamentales de los menores, considerando el estado del arte tecnológico y la evidencia científica disponible. El incumplimiento de este deber general genera responsabilidad independientemente de la infracción de obligaciones específicas de la presente ley.

ARTÍCULO 20°. ***Obligación de integración.*** Las plataformas digitales reguladas que operen o sean accesibles desde el territorio argentino deben integrar el protocolo del SINAVE dentro de los plazos del artículo 63. Hasta la plena operatividad del SINAVE, deben implementar mecanismos propios de verificación conforme estándares mínimos que establezca la Autoridad de Aplicación.

ARTÍCULO 21°. ***Deber de detección proactiva.*** Las plataformas deben implementar sistemas de detección proactiva de cuentas de menores no verificadas, incluyendo análisis conductual no intrusivo que no implique procesamiento de datos biométricos ni contenido de comunicaciones privadas, alertas ante indicadores de edad incompatible y mecanismos de reporte por otros usuarios.

ARTÍCULO 22°. ***Prohibición de funcionalidades adictivas para menores.*** Las plataformas tienen prohibido ofrecer a cuentas de menores: a) Scroll infinito sin interrupciones programadas; b) Reproducción automática sin acción afirmativa del usuario; c) Notificaciones diseñadas para generar urgencia artificial; d) Métricas de validación social visibles, salvo configuración activa del menor mayor de dieciséis (16) años; e) Sistemas de recompensa intermitente vinculados al tiempo de permanencia; f) Filtros de realidad

aumentada que modifiquen rasgos faciales o corporales. La reglamentación podrá ampliar este listado conforme la evolución tecnológica y la evidencia científica disponible.

ARTÍCULO 23°. ***Prohibición de perfilamiento de menores.*** Las plataformas tienen prohibido: a) Elaborar perfiles conductuales, psicográficos o de intereses de menores con fines comerciales o de personalización; b) Utilizar datos de menores para entrenar modelos de inteligencia artificial; c) Compartir, vender o transferir datos de menores a terceros; d) Realizar publicidad dirigida basada en inferencias sobre personalidad, estado emocional o vulnerabilidades del menor.

ARTÍCULO 24°. ***Deber de moderación reforzada.*** Las plataformas deben implementar moderación reforzada para menores que: a) Impida la exposición a contenido que promueva autolesiones, suicidio, trastornos alimentarios, consumo de sustancias o violencia; b) Detecte y bloquee intentos de contacto con fines de abuso sexual de menores (grooming); c) Implemente canales de denuncia con respuesta dentro de los plazos que establezca la reglamentación; d) Ofrezca recursos de ayuda ante contenido potencialmente dañino.

TÍTULO V — RÉGIMEN DE PLATAFORMAS DE MUY GRAN ESCALA (PMGE)

ARTÍCULO 25°. ***Clasificación.*** La Autoridad de Aplicación clasifica como Plataforma de Muy Gran Escala (PMGE) a toda plataforma digital regulada que cumpla al menos uno de los siguientes criterios: a) Cuente con más de cuatro millones (4.000.000) de usuarios activos mensuales en la República Argentina; b) Cuente con más de un millón (1.000.000) de usuarios menores de dieciocho (18) años en la República Argentina; c) Represente, por la naturaleza de sus funcionalidades de diseño, un riesgo sistémico significativo para menores conforme evaluación motivada de la Autoridad de Aplicación. La clasificación debe ser motivada, notificada a la plataforma y es recurrible conforme el artículo 47. La Autoridad publica y actualiza semestralmente el listado de PMGE.

ARTÍCULO 26°. ***Evaluación de riesgo sistémico.*** Las PMGE deben realizar y presentar ante la Autoridad de Aplicación una evaluación de riesgo sistémico anual que analice, como mínimo: a) Los riesgos derivados del diseño de los sistemas de recomendación algorítmica sobre la salud mental de menores; b) Los riesgos derivados de las

funcionalidades de interacción social para la seguridad de menores; c) Los riesgos de difusión de contenido ilegal o dañino para menores a través de la plataforma; d) Los riesgos derivados de la recopilación y tratamiento de datos de menores; e) Los efectos previsibles de la plataforma sobre la autonomía cognitiva y los derechos fundamentales de menores. La evaluación debe realizarse conforme metodología independiente y siguiendo los lineamientos del test de proporcionalidad del artículo 5.

ARTÍCULO 27°. ***Plan de mitigación.*** Sobre la base de la evaluación de riesgo, cada PMGE debe elaborar y ejecutar un plan de mitigación anual que incluya medidas concretas para cada riesgo identificado, cronograma de implementación, indicadores de efectividad y responsable interno de ejecución. El plan y su grado de cumplimiento son auditables por la Autoridad de Aplicación y por los auditores independientes del artículo 29.

ARTÍCULO 28°. ***Obligaciones reforzadas de PMGE.*** Además de las obligaciones generales del Título IV, las PMGE deben: a) Designar un responsable de protección de menores con jerarquía de dirección, con domicilio en la República Argentina; b) Someterse a auditoría algorítmica con la periodicidad reforzada que determine la reglamentación; c) Participar en el Comité de Diálogo Regulatorio previsto en el artículo 55.

ARTÍCULO 29°. ***Auditoría algorítmica.*** Las plataformas digitales reguladas están obligadas a someterse a auditoría algorítmica independiente con la periodicidad que determine la reglamentación, diferenciada para PMGE y demás plataformas, que evalúe: a) Cumplimiento de desactivación de funcionalidades adictivas; b) Eficacia de moderación de contenido dañino para menores; c) Ausencia de perfilamiento comercial de menores; d) Transparencia de sistemas de recomendación aplicados a menores; e) Integridad de la integración con el SINAVE. Los auditores son acreditados por la Autoridad de Aplicación conforme los requisitos que establezca la reglamentación. Los resultados se comunican a la Autoridad y se publican de forma resumida.

ARTÍCULO 30°. ***Informes de transparencia.*** Las plataformas publican periódicamente un Informe de Transparencia sobre Menores que incluya: a) Cuentas de menores verificadas por rango etario; b) Cuentas detectadas y eliminadas proactivamente; c) Denuncias recibidas categorizadas por tipo; d) Tiempo promedio de respuesta; e) Medidas implementadas; f) Resultados de auditorías algorítmicas. La periodicidad y

formato serán determinados por la reglamentación.

TÍTULO VI — DERECHOS DIGITALES DEL MENOR

ARTÍCULO 31°. ***Derechos del menor en plataformas digitales.*** Todo menor que utilice una plataforma digital regulada tiene derecho a: a) Recibir una explicación comprensible, adaptada a su edad, del funcionamiento de los sistemas de recomendación algorítmica que determinan el contenido que visualiza; b) Solicitar y obtener revisión humana de cualquier decisión automatizada que afecte su cuenta, incluyendo restricciones de contenido, suspensiones y bloqueos; c) Apelar ante la plataforma y, subsidiariamente, ante la Autoridad de Aplicación, cualquier decisión que restrinja su acceso o el uso de su cuenta; d) Solicitar la portabilidad de sus datos en formato interoperable y legible; e) Solicitar y obtener la eliminación completa de sus datos personales y contenido generado; f) Ser informado de manera clara y accesible sobre sus derechos conforme la presente ley; g) No ser sometido a decisiones exclusivamente automatizadas que produzcan efectos significativos sobre su persona.

ARTÍCULO 32°. ***Ejercicio de derechos.*** Los derechos del artículo anterior pueden ser ejercidos: a) Directamente por el menor mayor de dieciséis (16) años; b) Por el menor de trece (13) a quince (15) años con asistencia de su padre, madre o tutor; c) Por el padre, madre o tutor en representación del menor de trece (13) años. La plataforma debe resolver las solicitudes dentro del plazo que establezca la reglamentación y comunicar la respuesta de manera accesible al menor.

TÍTULO VII — PROTECCIÓN DE DATOS Y PRIVACIDAD

ARTÍCULO 33°. ***Principio de minimización estricta.*** En el contexto de la verificación de edad: a) Solo se procesa el dato estrictamente necesario; b) Ningún dato personal se transfiere a la plataforma; c) El resultado es exclusivamente una respuesta binaria; d) Los datos se eliminan inmediatamente después del proceso, salvo el token almacenado localmente.

ARTÍCULO 34°. ***Prohibición de uso secundario.*** Los datos generados en la verificación de edad no pueden utilizarse para publicidad, marketing, perfilamiento, entrenamiento de

inteligencia artificial, vigilancia o rastreo de actividad en línea, ni cualquier finalidad distinta de la verificación.

ARTÍCULO 35°. ***Protección de datos biométricos.*** Si se utiliza estimación de edad por medios biométricos: a) El procesamiento debe ser exclusivamente local en el dispositivo; b) Ninguna imagen, plantilla biométrica ni derivado se transmite fuera del dispositivo; c) Los datos biométricos se eliminan dentro de los plazos que establezca la reglamentación; d) El menor o su representante puede optar por verificación mediante token en lugar de estimación biométrica.

ARTÍCULO 36°. ***Evaluación de impacto.*** Toda plataforma debe realizar una Evaluación de Impacto en la Protección de Datos específica para menores, conforme lineamientos de la Autoridad de Aplicación y el organismo competente en materia de protección de datos personales. Se actualiza anualmente y su resumen ejecutivo es público.

ARTÍCULO 37°. ***Acceso a datos para investigación científica.*** Las plataformas digitales reguladas deben proveer acceso seguro, anonimizado y auditado a conjuntos de datos relevantes para la investigación científica sobre el impacto de las plataformas en menores, conforme las siguientes condiciones: a) El acceso se otorga a investigadores afiliados a instituciones del sistema científico-tecnológico nacional o a organismos internacionales reconocidos, previa acreditación ante la Autoridad de Aplicación; b) Los datos se proporcionan en formato anonimizado irreversible conforme los estándares que establezca la Autoridad de Aplicación; c) Los investigadores asumen compromiso de confidencialidad y uso exclusivamente científico; d) Las plataformas no pueden condicionar el acceso a restricciones sobre la publicación de resultados; e) La Autoridad de Aplicación publica un catálogo de conjuntos de datos disponibles y un protocolo de solicitud estandarizado; f) Las PMGE tienen obligación de responder a las solicitudes dentro del plazo que establezca la reglamentación. El incumplimiento de esta obligación constituye infracción grave.

TÍTULO VIII — EDUCACIÓN Y ALFABETIZACIÓN DIGITAL

ARTÍCULO 38°. ***Programa PROALFA-D.*** Créase el Programa Nacional de Alfabetización Digital para Familias (PROALFA-D), a cargo del Ministerio de Educación en coordinación con la Autoridad de Aplicación, para: a) Capacitar a padres, madres y tutores en control

parental y verificación de edad; b) Promover comprensión de riesgos y beneficios de plataformas digitales; c) Difundir estrategias de mediación parental activa; d) Desarrollar materiales adaptados a distintos contextos socioeconómicos y culturales.

ARTÍCULO 39°. ***Contenido curricular.*** El Ministerio de Educación incorporará en los Núcleos de Aprendizajes Prioritarios contenidos de ciudadanía digital, pensamiento crítico frente a contenido algorítmico y autogestión del tiempo en entornos digitales.

ARTÍCULO 40°. ***Campaña de concientización.*** La Autoridad de Aplicación implementará una campaña permanente de concientización sobre derechos de menores en el entorno digital, riesgos de funcionalidades adictivas y herramientas de protección disponibles.

TÍTULO IX — RÉGIMEN SANCIONATORIO

Capítulo 1 — Infracciones

ARTÍCULO 41°. ***Infracciones leves.*** Constituyen infracciones leves: a) Incumplimiento de plazos de publicación del Informe de Transparencia; b) Demora en respuesta a denuncias dentro de los márgenes que establezca la reglamentación.

ARTÍCULO 42°. ***Infracciones graves.*** Constituyen infracciones graves: a) Omisión de integrar el protocolo del SINAVE en plazo; b) Incumplimiento de la modalidad protegida; c) Omisión de auditoría algorítmica; d) Omisión de detección proactiva; e) Incumplimiento de reverificación; f) Incumplimiento de la obligación de acceso a datos para investigación del artículo 37; g) Incumplimiento de las obligaciones de evaluación de riesgo o plan de mitigación por las PMGE.

ARTÍCULO 43°. ***Infracciones muy graves.*** Constituyen infracciones muy graves: a) Permitir deliberada o negligentemente cuentas de menores de trece (13) años; b) Perfilamiento comercial de menores; c) Uso de datos de verificación para fines distintos de los previstos en esta ley; d) Transmisión o almacenamiento de datos biométricos fuera del dispositivo; e) Obstrucción de la fiscalización de la Autoridad de Aplicación; f) Reincidencia en infracciones graves; g) Incumplimiento del deber de diligencia reforzada que resulte en daño comprobado a menores.

Capítulo 2 — Sanciones

ARTÍCULO 44°. ***Escala sancionatoria.*** Las infracciones se sancionan conforme la

siguiente escala: a) Leves: apercibimiento y/o multa de cien (100) a mil (1.000) Salarios Mínimos, Vitales y Móviles (SMVM); b) Graves: multa de mil (1.000) a diez mil (10.000) SMVM; c) Muy graves: multa de diez mil (10.000) a cien mil (100.000) SMVM, y/o suspensión de operación por hasta noventa (90) días, y/o inhabilitación para contratar con el Estado por hasta cinco (5) años.

ARTÍCULO 45°. ***Criterios de graduación.*** Para la graduación de las sanciones se consideran: a) Gravedad y duración de la infracción; b) Número de menores afectados; c) Intencionalidad o negligencia; d) Cooperación con la Autoridad de Aplicación; e) Capacidad económica del infractor; f) Beneficios obtenidos por la infracción; g) Reincidencia; h) Resultado del test de proporcionalidad del artículo 5; i) Medidas correctivas adoptadas por la plataforma antes o durante el procedimiento.

Capítulo 3 — Régimen de ejecución para plataformas extranjeras

ARTÍCULO 46°. ***Representante legal obligatorio.*** Toda plataforma digital regulada con sede fuera de la República Argentina que cuente con más de un millón (1.000.000) de usuarios en el territorio nacional debe designar un representante legal con domicilio en la Argentina, con poder suficiente para: a) Recibir comunicaciones y notificaciones de la Autoridad de Aplicación y de los tribunales argentinos; b) Responder a requerimientos de información; c) Comparecer en procedimientos administrativos y judiciales. El incumplimiento de esta obligación constituye infracción grave y habilita la adopción de las medidas del artículo 48.

ARTÍCULO 47°. ***Garantías de debido proceso.*** En todo procedimiento sancionatorio o de ejecución previsto en la presente ley se garantiza: a) Notificación fehaciente del inicio del procedimiento y de los cargos formulados; b) Acceso irrestricto al expediente administrativo; c) Plazo de descargo no inferior a quince (15) días hábiles, prorrogable por causa justificada; d) Derecho a ofrecer y producir prueba, incluyendo prueba pericial técnica; e) Resolución motivada que incluya análisis explícito del test de proporcionalidad del artículo 5; f) Recurso de reconsideración ante la Autoridad de Aplicación dentro de los diez (10) días hábiles de notificada la resolución; g) Recurso directo ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal dentro de los treinta (30) días hábiles de notificada la resolución del recurso de reconsideración o vencido el plazo para resolverlo. El recurso directo tiene efecto suspensivo respecto de las sanciones pecuniarias. Las medidas de suspensión de

operación o bloqueo no se ejecutan hasta que adquieran firmeza, salvo riesgo inminente debidamente fundado conforme el artículo 48.

ARTÍCULO 48°. ***Medidas de ejecución reforzada.*** Cuando una plataforma digital regulada con sede fuera de la República Argentina incumpla las obligaciones de la presente ley y no designe representante legal conforme el artículo 46, la Autoridad de Aplicación puede, además de las sanciones ordinarias, adoptar las siguientes medidas conforme un régimen estricto de progresividad: a) Requerimiento de cumplimiento con plazo cierto no inferior a treinta (30) días corridos, notificado por todos los medios disponibles, incluyendo notificación electrónica al domicilio digital de la plataforma; b) Imposición de astreintes diarias hasta el efectivo cumplimiento; c) Orden de bloqueo progresivo del acceso desde el territorio nacional, implementada a través de los proveedores de servicios de Internet, previa autorización judicial del juez federal competente; d) Comunicación a las autoridades regulatorias de otros Estados con acuerdos de cooperación vigentes. Cada medida del inciso precedente solo procede ante el fracaso debidamente acreditado de la medida anterior. La medida del inciso c) solo procede ante incumplimiento reiterado y sistemático de las obligaciones de la presente ley que genere riesgo grave para los derechos de menores, previa autorización judicial mediante resolución fundada que analice expresamente el test de proporcionalidad del artículo 5, la afectación de derechos de usuarios adultos y la existencia de medidas alternativas menos restrictivas. La resolución judicial es apelable con efecto suspensivo. Cuando exista riesgo inminente, grave y debidamente fundado para la integridad física o psíquica de menores, la Autoridad de Aplicación puede solicitar al juez federal competente medidas cautelares urgentes. En tal caso, debe otorgarse audiencia a la plataforma dentro de los cinco (5) días hábiles siguientes, bajo apercibimiento de caducidad de la medida.

ARTÍCULO 49°. ***Destino de las multas.*** El producido de las multas se destina: cincuenta por ciento (50%) al financiamiento del SINAVE y cincuenta por ciento (50%) al PROALFA-D.

TÍTULO X — AUTORIDAD DE APLICACIÓN Y GOBERNANZA

Capítulo 1 — Agencia Nacional de Protección Digital de Menores

ARTÍCULO 50°. ***Creación.*** Créase la Agencia Nacional de Protección Digital de Menores (ANPDM) como organismo desconcentrado en la órbita de la Jefatura de Gabinete de Ministros, con independencia técnica, autonomía funcional, personería jurídica propia y autarquía financiera. La ANPDM es la Autoridad de Aplicación de la presente ley.

ARTÍCULO 51°. ***Dirección.*** La ANPDM será conducida por un Directorio integrado por cinco (5) miembros: un (1) Director Ejecutivo y cuatro (4) Directores, designados por el Poder Ejecutivo Nacional previo concurso público de antecedentes y oposición. Los candidatos deberán acreditar título universitario de grado, antecedentes profesionales o académicos relevantes en al menos una de las siguientes áreas: derecho digital, tecnologías de la información, protección de datos personales, derechos de la niñez o políticas públicas digitales, y no menos de diez (10) años de ejercicio profesional o académico en la materia.

ARTÍCULO 52°. ***Mandato y remoción.*** Los miembros del Directorio son designados por un mandato de cinco (5) años, renovable por un (1) período adicional. El mandato es escalonado: en la primera designación, dos (2) Directores serán nombrados por tres (3) años y los restantes por cinco (5) años. Los miembros del Directorio solo pueden ser removidos por el Poder Ejecutivo Nacional mediante acto fundado, por las siguientes causales: a) Mal desempeño de sus funciones; b) Comisión de delito doloso; c) Inhabilidad sobreviniente; d) Incumplimiento grave de los deberes del cargo. Previo a la remoción, debe garantizarse al miembro del Directorio el derecho de defensa, incluyendo descargo oral ante el funcionario que disponga la remoción.

ARTÍCULO 53°. ***Presupuesto protegido.*** La ANPDM elabora su propio presupuesto anual, que es remitido al Congreso de la Nación como anexo del presupuesto general de la Administración Nacional. Los fondos asignados a la ANPDM no pueden ser reasignados a otros organismos ni reducidos por debajo del nivel del ejercicio anterior sin autorización legislativa expresa. Constituyen recursos propios de la ANPDM: a) Las partidas que le asigne el presupuesto general; b) El cincuenta por ciento (50%) del producido de las multas conforme el artículo 49; c) Los aranceles por certificación de emisores privados y acreditación de auditores, conforme determine la reglamentación; d) Las donaciones, legados y subsidios que acepte el Directorio.

ARTÍCULO 54°. ***Funciones.*** Son funciones de la ANPDM: a) Administrar y supervisar el SINAVE; b) Establecer estándares técnicos y certificar proveedores y emisores; c)

Fiscalizar el cumplimiento de la presente ley; d) Instruir sumarios y aplicar sanciones conforme el Título IX; e) Publicar un Informe Anual de Situación; f) Coordinar con el RENAPER la emisión de tokens; g) Coordinar con el organismo competente en materia de protección de datos personales los aspectos relativos a privacidad, mediante convenio de articulación que delimite competencias y evite superposición; h) Coordinar con el Ministerio de Educación el PROALFA-D; i) Acreditar auditores independientes; j) Mantener el Registro de Plataformas Reguladas; k) Clasificar y actualizar el listado de PMGE; l) Administrar el sandbox regulatorio del artículo 58; m) Publicar el catálogo de datos para investigación del artículo 37; n) Articular con el Ente Nacional de Comunicaciones (ENACOM) las medidas que requieran intervención sobre prestadores de servicios de telecomunicaciones; o) Promover la cooperación internacional en la materia.

ARTÍCULO 55°. ***Incompatibilidades.*** Los miembros del Directorio no pueden: a) Tener interés directo o indirecto en plataformas digitales reguladas por la presente ley; b) Ejercer otra función pública, salvo la docencia; c) Realizar actividad profesional vinculada a la industria tecnológica regulada por la presente ley, durante su mandato y hasta dos (2) años después de su cese. La violación de estas incompatibilidades es causal de remoción.

Capítulo 2 — Órganos consultivos

ARTÍCULO 56°. ***Consejo Asesor.*** Créase el Consejo Asesor del SIVEM, de carácter consultivo y honorario, integrado por: a) Un representante del RENAPER; b) Un representante del organismo competente en materia de protección de datos personales; c) Un representante del Ministerio de Educación; d) Un representante del Ministerio de Salud; e) Un representante de la Defensoría del Pueblo de la Nación; f) Dos representantes de organizaciones de derechos de la niñez con reconocida trayectoria; g) Dos representantes del sector académico con especialización en tecnología o derechos digitales; h) Un representante del sector tecnológico nacional; i) Dos representantes de organizaciones de jóvenes de dieciséis (16) a dieciocho (18) años.

ARTÍCULO 57°. ***Comité de Diálogo Regulatorio.*** Créase el Comité de Diálogo Regulatorio, convocado semestralmente por la ANPDM, como espacio de interlocución entre la Autoridad, las PMGE, las organizaciones de la sociedad civil y el sector académico, para: a) Analizar los resultados de los indicadores de efectividad; b) Evaluar

la proporcionalidad de las medidas vigentes; c) Identificar riesgos emergentes; d) Proponer mejoras regulatorias. Las conclusiones del Comité son públicas y no vinculantes.

Capítulo 3 — Defensor del Menor Digital

ARTÍCULO 58°. ***Defensor del Menor Digital.*** Créase la figura del Defensor del Menor Digital dentro de la ANPDM, designado por el Directorio mediante concurso público, con las siguientes funciones: a) Recibir y tramitar denuncias de menores y familias; b) Representar el interés del menor en procedimientos administrativos ante la ANPDM; c) Emitir recomendaciones al Directorio; d) Elaborar un informe semestral sobre el estado de los derechos de menores en entornos digitales, que se remite al Congreso de la Nación.

TÍTULO XI — INNOVACIÓN, MÉTRICAS Y MEJORA CONTINUA

ARTÍCULO 59°. ***Sandbox regulatorio.*** Créase el Sandbox Regulatorio de Protección Digital de Menores, administrado por la ANPDM, con el objeto de: a) Permitir el desarrollo y testeo controlado de nuevas tecnologías de verificación de edad; b) Evaluar soluciones de privacidad mejorada para la protección de menores; c) Experimentar con modelos de moderación de contenido basados en inteligencia artificial; d) Desarrollar herramientas de control parental innovadoras. Los participantes operan bajo condiciones controladas definidas por la ANPDM, con protecciones reforzadas para los menores involucrados. La reglamentación determinará la duración de los ciclos, los requisitos de participación, las condiciones de publicación de resultados y las protecciones específicas aplicables.

ARTÍCULO 60°. ***Indicadores de efectividad.*** La ANPDM establece y publica indicadores clave de efectividad que las plataformas deben medir y reportar, conforme los lineamientos que determine la reglamentación. Los indicadores deben incluir, como mínimo, métricas relativas a la reducción de exposición de menores a contenido dañino, patrones de tiempo de uso, tasas de detección de cuentas no verificadas e intentos de grooming, tiempos de respuesta a denuncias y tasas de verificación mediante token. El incumplimiento de metas de efectividad razonables establecidas por la ANPDM constituye elemento agravante en la graduación de sanciones.

ARTÍCULO 61°. ***Investigación.*** La ANPDM promueve la investigación sobre: a) Los efectos de las plataformas digitales en la salud mental de menores argentinos; b) La eficacia de las medidas de la presente ley; c) El desarrollo de tecnologías de verificación respetuosas de la privacidad; d) Los patrones de uso digital de menores en la Argentina.

ARTÍCULO 62°. ***Revisión periódica.*** La ley y su reglamentación se someten a revisión integral cada tres (3) años, sobre la base de los Informes Anuales de Situación, la evolución de la evidencia científica, el desarrollo tecnológico, la experiencia comparada internacional y los resultados de los indicadores de efectividad y del sandbox regulatorio. La ANPDM eleva al Congreso de la Nación un informe con recomendaciones de reforma.

TÍTULO XII — DISPOSICIONES COMPLEMENTARIAS

ARTÍCULO 63°. ***Acción judicial colectiva.*** Las asociaciones de defensa del consumidor, organizaciones de derechos de la niñez, el Ministerio Público Fiscal y la Defensoría del Pueblo están legitimados para interponer acciones colectivas por incumplimientos de la presente ley.

ARTÍCULO 64°. ***Prohibición de represalias.*** Las plataformas digitales reguladas tienen prohibido adoptar medidas técnicas, comerciales o de cualquier naturaleza en represalia contra usuarios, investigadores, organizaciones o representantes que ejerzan derechos o presenten denuncias conforme la presente ley.

TÍTULO XIII — DISPOSICIONES TRANSITORIAS Y FINALES

ARTÍCULO 65°. ***Reglamentación.*** El Poder Ejecutivo reglamentará la presente ley dentro de los ciento ochenta (180) días de su publicación.

ARTÍCULO 66°. ***Puesta en funcionamiento de la ANPDM.*** El Poder Ejecutivo Nacional pondrá en funcionamiento la ANPDM dentro de los ciento veinte (120) días de la publicación de la presente ley. Dentro de los sesenta (60) días siguientes a su puesta en funcionamiento, el Directorio dictará su reglamento interno de funcionamiento.

ARTÍCULO 67°. ***Desarrollo del SINAVE.*** La ANPDM, en coordinación con el RENAPER, desarrollará la infraestructura del SINAVE dentro de los doce (12) meses posteriores a

la reglamentación.

ARTÍCULO 68°. ***Primer listado de PMGE.*** La ANPDM publicará el primer listado de PMGE dentro de los noventa (90) días posteriores a la reglamentación.

ARTÍCULO 69°. ***Período de adecuación de PMGE.*** Las plataformas clasificadas como PMGE tendrán un plazo de ciento ochenta (180) días desde su clasificación para presentar la primera evaluación de riesgo sistémico y el plan de mitigación.

ARTÍCULO 70°. ***Activación del sandbox.*** La ANPDM convocará al primer ciclo del sandbox regulatorio dentro de los doce (12) meses de la reglamentación.

ARTÍCULO 71°. ***Implementación escalonada.*** La presente ley se implementa conforme el siguiente cronograma: a) Seis (6) meses de la reglamentación: modalidad protegida y prohibición de funcionalidades adictivas para PMGE; b) Doce (12) meses: plena operatividad del SINAVE y obligación de integración para PMGE; c) Dieciocho (18) meses: extensión de todas las obligaciones al resto de plataformas reguladas.

ARTÍCULO 72°. ***Régimen transitorio de verificación.*** Hasta la plena operatividad del SINAVE, las plataformas deben implementar como mínimo: a) Autodeclaración con verificación cruzada contra bases públicas, con eliminación inmediata de datos verificados; b) Estimación de edad conforme el artículo 15; c) Consentimiento parental verificable mediante los mecanismos que establezca la reglamentación.

ARTÍCULO 73°. ***Presupuesto.*** Autorízanse las adecuaciones presupuestarias necesarias para la implementación de la presente ley. A partir del ejercicio siguiente a la puesta en funcionamiento de la ANPDM, los gastos se incorporan al presupuesto general de la Administración Nacional.

ARTÍCULO 74°. ***Normas complementarias.*** La presente ley es complementaria de las Leyes 26.061, 25.326 y 24.240, o las que en el futuro las reemplacen, y se interpreta conforme la Convención sobre los Derechos del Niño.

ARTÍCULO 75°. ***Invitación a las provincias.*** Invítase a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a la presente ley y a adoptar las medidas necesarias para su efectiva implementación en sus jurisdicciones.

ARTÍCULO 76°. ***Vigencia.*** La presente ley entra en vigencia al día siguiente de su publicación en el Boletín Oficial.

ARTÍCULO 77°. ***Comuníquese al Poder Ejecutivo Nacional.***

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

El presente proyecto de ley tiene por objeto establecer un sistema integral de verificación de edad para menores en entornos digitales que garantice simultáneamente la protección efectiva de niños, niñas y adolescentes frente a los riesgos documentados de las plataformas digitales, el respeto irrestricto del derecho a la privacidad y a la protección de datos personales, la soberanía tecnológica del Estado argentino en la gestión de la identidad digital de sus ciudadanos, y la viabilidad técnica de su implementación a escala nacional.

I. LA EVIDENCIA CIENTÍFICA: UN CONSENSO CONVERGENTE

La evidencia científica sobre los daños que las redes sociales generan en la salud mental de niños y adolescentes proviene de múltiples fuentes independientes y de alto nivel, configurando un consenso convergente que justifica la intervención legislativa:

1. El Cirujano General de los Estados Unidos, Dr. Vivek Murthy, publicó en mayo de 2023 el Advisory on Social Media and Youth Mental Health, en el que concluyó que "la ciencia actual no puede determinar que las redes sociales sean suficientemente seguras para niños y adolescentes". El Advisory documentó que los adolescentes que pasan más de tres horas diarias en redes sociales duplican el riesgo de depresión y ansiedad (U.S. Surgeon General's Advisory, "Social Media and Youth Mental Health", mayo 2023; disponible en https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html).

2. Un experimento natural publicado en la American Economic Review demostró que la introducción escalonada de Facebook en universidades de Estados Unidos se asoció con un incremento del 9% en los diagnósticos de depresión y del 12% en los de trastorno de ansiedad generalizada entre estudiantes. Este estudio es particularmente relevante por su diseño cuasiexperimental, que permite inferencias causales más robustas que los estudios correlacionales (Braghieri, L., Levy, R. y Makarin, A., "Social Media and Mental Health", American Economic Review, vol. 112, n.° 11, noviembre 2022, pp. 3660-3693; DOI: 10.1257/aer.20211218).

3. Un estudio longitudinal publicado en JAMA con una cohorte de más de 6.000 niños del estudio ABCD (Adolescent Brain Cognitive Development) demostró que el uso

creciente de redes sociales predice peor desempeño en lectura, vocabulario y memoria episódica, controlando por variables socioeconómicas y demográficas (Nagata, J.M. et al., “Association of Social Media Use with Cognitive Development in Children”, JAMA, 2025; DOI: 10.1001/jama.2024.27669).

4. La Asociación Americana de Psicología emitió en mayo de 2023 un Health Advisory on Social Media Use in Adolescence, con recomendaciones específicas para limitar la exposición de menores a funcionalidades adictivas, perfilamiento comercial y contenido dañino. El Advisory identifica que el uso de redes sociales no es inherentemente perjudicial ni beneficioso, pero que ciertas funcionalidades de diseño —particularmente las de refuerzo variable— generan patrones de uso compulsivo en adolescentes (APA, “Health Advisory on Social Media Use in Adolescence”, mayo 2023; disponible en https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use).

5. El World Happiness Report 2026, publicado por el Sustainable Development Solutions Network, dedicó un capítulo completo al impacto de las redes sociales en el bienestar de menores, concluyendo que los efectos negativos se producen a escala poblacional y no son explicables exclusivamente por vulnerabilidades individuales previas (World Happiness Report 2026, cap. 5; disponible en https://worldhappiness.report).

6. La investigación de eSafety Australia (2025-2026) documentó los patrones de riesgo específicos para menores en plataformas digitales en el contexto de la implementación de la ley australiana, identificando que las funcionalidades adictivas, el perfilamiento algorítmico y la exposición a contenido de autolesiones constituyeron los principales vectores de daño (eSafety Commissioner, informes anuales 2025-2026; disponible en https://www.esafety.gov.au).

7. Los trabajos de Jonathan Haidt (The Anxious Generation, Penguin Press, 2024) y Jean Twenge (iGen, Atria Books, 2017; Generations, Atria Books, 2023) documentan longitudinalmente la correlación entre la adopción masiva de smartphones y redes sociales y el deterioro de indicadores de salud mental adolescente en países de la OCDE.

Esta convergencia de fuentes —un advisory del Cirujano General, estudios experimentales y longitudinales en las principales revistas científicas, pronunciamientos de la principal asociación profesional de psicología, informes internacionales sobre bienestar y datos de reguladores nacionales— configura un nivel de evidencia que

satisface los estándares de la Corte Suprema de Justicia de la Nación para la justificación de restricciones razonables a derechos constitucionales (doctrina “Fallos” 327:3677, “Asociación Benghalensis”, y concordantes).

II. LAS LECCIONES DEL MODELO AUSTRALIANO

Australia implementó en diciembre de 2025 la Online Safety Amendment (Social Media Minimum Age) Act 2024, la primera prohibición nacional de acceso a redes sociales para menores de 16 años. Tras un año de vigencia, la experiencia reveló problemas que este proyecto busca superar:

a) La prohibición absoluta sin excepciones ni consentimiento parental desconoce el principio de autonomía progresiva del menor consagrado en el artículo 5 de la Convención sobre los Derechos del Niño y en el artículo 3 de la Ley 26.061 argentina.

b) La delegación de la verificación a las propias plataformas, sin un estándar estatal unificado, generó fragmentación técnica y facilitó la evasión mediante suplantación de identidad y VPN.

c) La exclusión de menores de redes de apoyo legítimas en materia de salud mental, educación y comunidad, especialmente para poblaciones vulnerables, fue señalada por UNICEF Australia, Amnesty International y académicos publicados en The Lancet Digital Health como una consecuencia desproporcionada de la medida (The Lancet Digital Health, editorial, vol. 7, 2025).

d) Incidentes de seguridad, como la filtración de datos de verificación que afectó a decenas de miles de usuarios, pusieron de manifiesto los riesgos de sistemas centralizados de verificación gestionados por las propias plataformas.

El SIVEM toma nota de estas lecciones y las supera mediante: un régimen escalonado por edad (no una prohibición binaria), verificación soberana (no delegada a plataformas), arquitectura federada descentralizada (no un punto único de fallo) y preservación explícita del acceso a plataformas educativas, de salud y de apoyo.

III. EL MODELO EUROPEO Y ESTÁNDARES OCDE

La Unión Europea ha desarrollado el marco regulatorio más sofisticado del mundo en materia de gobernanza digital. Este proyecto se alinea expresamente con tres instrumentos clave:

a) El Digital Services Act (Reglamento UE 2022/2065), que introduce la clasificación de plataformas de muy gran escala (Very Large Online Platforms, VLOP) con obligaciones diferenciadas de evaluación de riesgo sistémico, auditoría algorítmica independiente y acceso a datos para investigación. El concepto de PMGE del SIVEM replica esta arquitectura regulatoria.

b) El Reglamento eIDAS 2.0 (Reglamento UE 2024/1183), que establece el marco para la European Digital Identity Wallet y las credenciales verificables interoperables. El diseño del SINAVE se alinea con estos estándares para garantizar interoperabilidad futura.

c) La Resolución del Parlamento Europeo de noviembre de 2025 sobre protección de menores en entornos digitales, que propuso un modelo de acceso escalonado por edad con consentimiento parental para el rango de 13 a 15 años, prohibición de funcionalidades adictivas y protección contra explotación comercial de menores.

La OCDE, en su Recommendation of the Council on Children in the Digital Environment (2021, OECD/LEGAL/0389) y en los documentos complementarios del Working Party on Digital Economy Policy, recomienda expresamente: enfoques basados en riesgo y proporcionalidad, evaluaciones de impacto obligatorias, sandboxes regulatorios para innovación, y métricas de efectividad como herramientas de regulación basada en resultados. El SIVEM incorpora cada uno de estos elementos.

IV. LA VENTAJA ESTRATÉGICA ARGENTINA

La Argentina cuenta con una infraestructura de identidad digital a través del RENAPER y la plataforma Mi Argentina que permite construir un sistema soberano de verificación de edad sin depender de soluciones tecnológicas extranjeras. El Documento Nacional de Identidad digital, el Sistema de Identidad Digital (SID) y la firma digital del Estado argentino constituyen la base técnica sobre la cual se construye el SINAVE.

El proyecto propone una arquitectura federada con tokens criptográficos basados en pruebas de conocimiento cero (Zero-Knowledge Proofs), donde el Estado actúa como raíz de confianza pero admite múltiples emisores certificados —públicos y privados—, evitando tanto la centralización excesiva como la dependencia de plataformas extranjeras. Este diseño se inspira en el modelo de identidad autosoberana (self-sovereign identity) promovido por el W3C a través de los estándares de Verifiable Credentials y Decentralized Identifiers (DIDs), y en el proyecto euCONSENT de la Unión

Europea para verificación de edad con preservación de privacidad.

V. DISEÑO INSTITUCIONAL: LA AGENCIA NACIONAL DE PROTECCIÓN DIGITAL DE MENORES

El proyecto crea la Agencia Nacional de Protección Digital de Menores (ANPDM) como organismo desconcentrado con independencia técnica, autonomía funcional y presupuesto protegido. El diseño institucional se inspira en los modelos exitosos de reguladores independientes argentinos, adaptados a la especificidad de la materia:

a) Directorio plural de cinco miembros designados por concurso público, con mandato fijo de cinco años, escalonado, para garantizar continuidad institucional más allá de los ciclos políticos.

b) Remoción solo por causales taxativas y con garantía de defensa, siguiendo la doctrina de la Corte Suprema sobre estabilidad de funcionarios de organismos de control ("Ángel Estrada", Fallos 328:651, y concordantes).

c) Presupuesto protegido con cláusula de no reducción sin autorización legislativa, complementado con recursos propios provenientes de multas, aranceles de certificación y otras fuentes.

d) Régimen de incompatibilidades estricto con "puerta giratoria" de dos años post-cese, para prevenir captura regulatoria.

e) Articulación explícita con el organismo de protección de datos personales y con ENACOM, mediante convenios que delimitan competencias y evitan superposición.

VI. BLINDAJE CONSTITUCIONAL DEL ENFORCEMENT

El régimen sancionatorio y de ejecución ha sido diseñado con especial atención al blindaje constitucional, anticipando las previsibles impugnaciones de plataformas extranjeras:

a) Test de proporcionalidad tripartito explícito (idoneidad, necesidad, proporcionalidad estricta) como requisito obligatorio de cada acto regulatorio, con carga de documentación para la Autoridad y derecho de impugnación para las plataformas (artículo 5).

b) Régimen estricto de progresividad para las medidas de ejecución: requerimiento,

astreintes, bloqueo. Cada medida solo procede ante el fracaso acreditado de la anterior (artículo 48).

c) El bloqueo —medida más restrictiva— requiere autorización judicial previa del juez federal competente, mediante resolución fundada que analice expresamente el test de proporcionalidad y la afectación de derechos de usuarios adultos (artículo 48, inciso c).

d) Plenas garantías de debido proceso: notificación, descargo, prueba —incluyendo pericial técnica—, resolución motivada, recurso de reconsideración y recurso directo ante la Cámara Contencioso Administrativo Federal, con efecto suspensivo para sanciones pecuniarias (artículo 47).

e) Las medidas cautelares urgentes solo proceden ante riesgo inminente para la integridad física o psíquica de menores, con audiencia obligatoria dentro de cinco días hábiles bajo apercibimiento de caducidad (artículo 48, último párrafo).

Este diseño satisface los estándares de la jurisprudencia de la Corte Suprema en materia de debido proceso administrativo (doctrina “Estrada”, “CIARA” y concordantes), de la Corte Interamericana de Derechos Humanos (OC-5/85 sobre libertad de expresión) y de los Principios de Manila sobre Responsabilidad de Intermediarios, reduciendo significativamente la superficie de impugnación constitucional.

VII. INNOVACIONES NORMATIVAS

El SIVEM introduce innovaciones que no se encuentran en ninguna legislación vigente comparada: (1) Test de proporcionalidad tripartito operativizado como requisito de cada acto regulatorio; (2) Clasificación de Plataformas de Muy Gran Escala con obligaciones diferenciadas; (3) Arquitectura federada del SINAVE con identidad autosoberana; (4) Derechos procesales del menor en el entorno digital (explicación algorítmica, revisión humana, apelación, portabilidad); (5) Enforcement con control judicial previo para medidas restrictivas; (6) Acceso obligatorio a datos para investigación; (7) Sandbox regulatorio; (8) Indicadores de efectividad obligatorios; (9) Agencia reguladora independiente con diseño anticaptura; (10) Deber general de diligencia reforzada como cláusula de adaptación futura.

VIII. ESTRUCTURA DE LA LEY

La ley se organiza en 13 títulos y 77 artículos: Título I (Disposiciones generales: objeto,

ámbito, definiciones, principios, test de proporcionalidad); Título II (Régimen de edad escalonado: prohibición para menores de 13, consentimiento parental de 13 a 15, acceso autónomo de 16 a 17, modalidad protegida); Título III (SINAVE: creación, arquitectura federada, funcionamiento, consentimiento parental, gratuidad, estimación subsidiaria, reverificación, interoperabilidad, código abierto); Título IV (Obligaciones de plataformas: deber de diligencia, integración, detección proactiva, funcionalidades adictivas, perfilamiento, moderación); Título V (Régimen PMGE: clasificación, evaluación de riesgo sistémico, plan de mitigación, obligaciones reforzadas, auditoría, transparencia); Título VI (Derechos digitales del menor); Título VII (Protección de datos: minimización, uso secundario, datos biométricos, evaluación de impacto, acceso para investigación); Título VIII (Educación: PROALFA-D, contenido curricular, campaña); Título IX (Régimen sancionatorio: infracciones, sanciones, representante legal, debido proceso, ejecución reforzada con control judicial); Título X (Autoridad de Aplicación: ANPDM como órgano desconcentrado con directorio por concurso, mandato fijo, remoción con causa, presupuesto protegido, incompatibilidades, Consejo Asesor, Comité de Diálogo, Defensor del Menor Digital); Título XI (Innovación: sandbox, indicadores, investigación, revisión periódica); Título XII (Disposiciones complementarias: acción colectiva, prohibición de represalias); Título XIII (Disposiciones transitorias: reglamentación, puesta en funcionamiento de la ANPDM, desarrollo del SINAVE, implementación escalonada en 18 meses para plataformas).

Las obligaciones de fabricantes de dispositivos, tiendas de aplicaciones, el régimen de etiquetado y la cooperación internacional se desarrollan en un proyecto de ley complementario que se presenta en forma conjunta, permitiendo su tratamiento diferenciado conforme la dinámica parlamentaria sin condicionar la aprobación de la ley núcleo.

Por todo lo expuesto, solicito a mis pares la aprobación del presente proyecto de ley.

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN