PROYECTO DE LEY

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

LEY DE RESPONSABILIDAD CIVIL POR DAÑOS DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

TÍTULO I — DISPOSICIONES GENERALES

ARTÍCULO 1º — *Objeto.* La presente ley tiene por objeto establecer el régimen de responsabilidad civil por daños causados por sistemas de inteligencia artificial y sistemas algorítmicos de toma de decisiones, a fin de garantizar la reparación efectiva de las personas afectadas, la seguridad jurídica de los operadores y el desarrollo responsable de la inteligencia artificial en la República Argentina.

ARTÍCULO 2º — *Ámbito de aplicación.* La presente ley se aplica a los daños causados por sistemas de inteligencia artificial que:

a) sean desarrollados, desplegados u operados en territorio argentino;

b) produzcan efectos dañosos en territorio argentino, con independencia del lugar de establecimiento de su operador;

c) sean utilizados para tomar o asistir decisiones que afecten a personas que se encuentren en la República Argentina;

d) siendo operados desde el exterior, procesen datos de personas domiciliadas en la República Argentina o dirijan sus servicios al mercado argentino, aun cuando no cuenten con establecimiento permanente en el país. A los efectos de este inciso, se considerará que un sistema de IA dirige sus servicios al mercado argentino cuando utilice idioma español rioplatense, acepte medios de pago locales, realice publicidad segmentada hacia usuarios argentinos, ofrezca contenidos o servicios adaptados a la jurisdicción argentina, o registre un

volumen significativo de usuarios o interacciones con personas domiciliadas en la República Argentina. Se presumirá la existencia de volumen significativo cuando el sistema cuente con más de cien mil (100.000) usuarios únicos mensuales domiciliados en el país, o cuando los ingresos atribuibles al mercado argentino superen el equivalente a diez mil (10.000) salarios mínimos vitales y móviles anuales. La Autoridad de Aplicación podrá actualizar estos umbrales mediante resolución fundada.

Se exceptúan:

a) los sistemas de IA utilizados exclusivamente con fines personales o domésticos;

b) los sistemas de IA utilizados exclusivamente con fines de defensa nacional, conforme legislación específica;

c) los daños cubiertos íntegramente por regímenes especiales de responsabilidad vigentes, salvo insuficiencia de la cobertura.

La presente ley constituye norma de orden público internacional en materia de protección de personas afectadas por sistemas de inteligencia artificial, y resultará aplicable con independencia de las cláusulas de elección de ley o jurisdicción que pudieran contener los contratos celebrados con los operadores.

ARTÍCULO 3º — *Definiciones.* A los efectos de la presente ley se entiende por:

a) Sistema de inteligencia artificial (sistema de IA): Todo sistema basado en máquinas que, a partir de los datos de entrada que recibe, genera resultados tales como predicciones, recomendaciones, decisiones, contenidos o acciones que pueden influir en entornos físicos o virtuales. Los sistemas de IA operan con distintos niveles de autonomía y pueden utilizar enfoques de aprendizaje automático, lógicos, estadísticos u otros métodos computacionales.

b) Sistema de IA de alto riesgo: Todo sistema de IA comprendido en alguna de las categorías del Anexo I de la presente ley. Sin perjuicio de las categorías enumeradas en el Anexo, un sistema de IA será igualmente considerado de alto riesgo cuando, por su naturaleza, alcance, contexto o fines, presente un riesgo elevado y concreto para la vida, integridad física, salud, patrimonio, derechos fundamentales o intereses esenciales de las personas, conforme los criterios que establezca la Autoridad de Aplicación mediante resolución fundada y previa consulta pública. La Autoridad de Aplicación actualizará el Anexo I con periodicidad bienal mediante resolución fundada, incorporando nuevas categorías cuando la evolución tecnológica lo requiera. La Autoridad de

Aplicación podrá declarar la intervención cautelar urgente sobre cualquier sistema de IA que presente riesgo sistémico inminente para la estabilidad financiera, la seguridad pública o los procesos democráticos, ordenando su suspensión temporal o la adopción de medidas correctivas inmediatas, con posterior control judicial dentro de las cuarenta y ocho (48) horas.

c) Operador: Toda persona humana o jurídica que desarrolle, despliegue, utilice, supervise o ponga a disposición de terceros un sistema de IA, ya sea en calidad de proveedor, implementador, usuario profesional o cualquier otra función en la cadena de valor del sistema.

d) Proveedor: Persona humana o jurídica que desarrolla o hace desarrollar un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca.

e) Implementador: Persona humana o jurídica que utiliza un sistema de IA bajo su autoridad en el marco de una actividad profesional.

f) Persona afectada: Toda persona humana que sufra un daño como consecuencia directa o indirecta del funcionamiento, resultado, omisión o defecto de un sistema de IA.

g) Daño: Todo menoscabo patrimonial o extrapatrimonial causado a una persona, incluyendo: daño físico, muerte o lesión corporal; daño psicológico; daño a la integridad mental o la continuidad psicológica; daño al patrimonio o intereses económicos; daño a los datos personales; daño derivado de discriminación algorítmica; y daño a la dignidad, la privacidad o la autonomía personal.

h) Resultado del sistema de IA: Toda predicción, recomendación, decisión, contenido, acción u omisión generada por un sistema de IA, incluyendo la ausencia de resultado cuando éste era esperable.

i) Deber de diligencia: Conjunto de obligaciones de cuidado, supervisión, mantenimiento, actualización y transparencia que los operadores deben observar según la clasificación de riesgo del sistema de IA, las normas técnicas aplicables, las instrucciones del proveedor y el estado del arte.

j) Opacidad del sistema: Imposibilidad o dificultad sustancial de explicar, auditar o reconstruir la lógica, los datos o los procesos internos que condujeron a un resultado específico del sistema de IA, sea por su complejidad computacional, por la negativa del operador a divulgar información, o por la ausencia de registros de funcionamiento.

k) Auditoría algorítmica: Proceso sistemático e independiente de evaluación de un sistema de IA para verificar su conformidad con los requisitos legales, técnicos y éticos aplicables.

l) Evaluación de conformidad: Procedimiento mediante el cual se verifica que un sistema de IA de alto riesgo cumple con los requisitos establecidos en la presente ley y su reglamentación antes de su puesta en servicio.

m) Sandbox de responsabilidad: Entorno regulatorio controlado que permite probar sistemas de IA innovadores bajo condiciones supervisadas conforme el Título VI de la presente ley.

n) Pricing regulatorio del riesgo: Sistema de diferenciación tarifaria de las primas de seguro obligatorio y aportes a fondos de garantía en función del nivel de riesgo efectivo del sistema de IA, su historial de siniestralidad y su grado de cumplimiento normativo, conforme el artículo 12 de la presente ley.

TÍTULO II — RÉGIMEN DE RESPONSABILIDAD

Capítulo 1 — Responsabilidad objetiva por sistemas de alto riesgo

ARTÍCULO 4º — *Responsabilidad objetiva del proveedor.* El proveedor de un sistema de IA de alto riesgo será objetivamente responsable por los daños causados por el funcionamiento, resultado, defecto u omisión del sistema, con independencia de la existencia de culpa.

El proveedor solo podrá eximirse acreditando:

a) que el daño fue causado exclusivamente por un hecho de la víctima;

b) caso fortuito o fuerza mayor externo al sistema y ajeno al riesgo creado por la tecnología;

c) que el sistema fue sustancialmente modificado por un tercero sin autorización ni conocimiento del proveedor, y que dicha modificación fue la causa exclusiva del daño;

d) que el riesgo específico que causó el daño era objetivamente no detectable conforme el estado del arte científico y técnico al momento de la puesta en servicio del sistema, y que el proveedor implementó un sistema de monitoreo post-mercado razonable que no permitió detectar el riesgo antes de la producción del daño.

La eximente del inciso d) no operará cuando el proveedor haya omitido realizar las evaluaciones de conformidad exigidas por la reglamentación, cuando haya recibido alertas de riesgo por parte de implementadores, usuarios o terceros y no haya adoptado medidas correctivas razonables, o cuando el sistema haya sido comercializado sin las instrucciones de uso y supervisión humana previstas en esta ley.

Se reconoce el crédito de cumplimiento (compliance credit): cuando el operador acredite haber obtenido certificaciones reconocidas, realizado auditorías periódicas conforme estándares internacionales, e implementado programas robustos de gestión de riesgos, tales circunstancias operarán como atenuantes en la graduación de la indemnización y de los daños punitivos, pudiendo reducir estos últimos hasta en un cincuenta por ciento (50%).

No constituye eximente la conformidad del sistema con normas técnicas, certificaciones o aprobaciones regulatorias al momento de su puesta en servicio.

ARTÍCULO 5º — *Responsabilidad del implementador de sistemas de alto riesgo.* El implementador de un sistema de IA de alto riesgo responderá solidariamente con el proveedor cuando:

a) utilice el sistema de manera contraria a las instrucciones del proveedor o fuera de su finalidad prevista;

b) omita implementar las medidas de supervisión humana requeridas;

c) no mantenga el sistema actualizado conforme las instrucciones del proveedor;

d) no adopte las medidas correctivas cuando conociera o debiera conocer un riesgo derivado del sistema.

El implementador que haya cumplido todas sus obligaciones de diligencia podrá repetir contra el proveedor por la totalidad de lo abonado.

ARTÍCULO 6º — *Responsabilidad solidaria en la cadena de valor.* Cuando el daño sea atribuible a múltiples operadores en la cadena de valor del sistema de IA, la responsabilidad será solidaria frente a la persona afectada, sin perjuicio de las acciones de regreso entre los corresponsables según su grado de participación en la causación del daño.

Capítulo 2 — Responsabilidad subjetiva por sistemas de riesgo no alto

ARTÍCULO 7º — *Responsabilidad basada en culpa.* El operador de un sistema de IA que no sea de alto riesgo responderá por los daños causados cuando haya incumplido el

deber de diligencia exigible conforme la naturaleza del sistema, el estado del arte, las normas técnicas aplicables y las circunstancias del caso.

Se considerará incumplimiento del deber de diligencia, entre otros supuestos:

a) la omisión de medidas razonables de supervisión o prueba;

b) la falta de actualización del sistema ante riesgos conocidos;

c) la omisión de información al usuario sobre las capacidades, limitaciones y riesgos del sistema.

ARTÍCULO 8º — *Presunción de causalidad.* Cuando una persona afectada acredite que:

a) el operador incumplió un deber de diligencia legalmente establecido o derivado del estado del arte; y

b) sea razonablemente probable que dicho incumplimiento haya causado el resultado dañoso del sistema de IA;

se presumirá, salvo prueba en contrario, que el incumplimiento fue la causa del daño.

Tratándose de sistemas de IA de alto riesgo, la presunción de causalidad operará cuando la persona afectada acredite únicamente que el sistema produjo un resultado que causó el daño, correspondiendo al operador acreditar que el daño no fue causado por el sistema.

ARTÍCULO 8º bis — *Inversión de la carga probatoria por opacidad.* Cuando concurran simultáneamente las siguientes circunstancias:

a) la existencia de un daño jurídicamente relevante;

b) que el daño haya sido producido en el contexto de la operación de un sistema de IA de alto riesgo; y

c) que el sistema presente opacidad en los términos del artículo 3º inciso j) de la presente ley;

se invertirá la carga de la prueba, correspondiendo al operador demostrar que obró con diligencia plena en el diseño, desarrollo, despliegue, monitoreo y supervisión del sistema, y que el daño no es atribuible a un defecto, sesgo, omisión o funcionamiento inadecuado del sistema de IA.

La inversión de la carga probatoria prevista en este artículo operará también cuando el operador haya incumplido la obligación de divulgación de evidencia ordenada

judicialmente conforme el artículo 9º, o cuando haya destruido, alterado u ocultado registros de funcionamiento del sistema.

El operador que pretenda invocar la ausencia de opacidad deberá acreditar que el sistema cuenta con mecanismos de explicabilidad, registros de funcionamiento completos y documentación técnica suficiente para reconstruir la lógica del resultado dañoso.

Capítulo 3 — Disposiciones comunes

ARTÍCULO 9º — ***Acceso a la información y divulgación de evidencia.*** Toda persona que alegue haber sufrido un daño causado por un sistema de IA tendrá derecho a solicitar judicialmente al operador la divulgación de la información necesaria para evaluar y sustanciar su reclamo, incluyendo:

a) la documentación técnica del sistema;

b) los registros de funcionamiento (logs) relevantes;

c) la descripción de los datos de entrada utilizados;

d) la explicación de la lógica del resultado específico que causó el daño;

e) las medidas de supervisión humana implementadas.

El juez ordenará la divulgación cuando la persona afectada acredite la existencia de un daño y la plausibilidad de la participación del sistema de IA en su causación.

La divulgación se limitará a lo necesario y proporcionado. El juez adoptará las medidas necesarias para proteger el secreto industrial, la propiedad intelectual y la información confidencial, sin que la protección del secreto industrial pueda impedir el acceso a información esencial para el ejercicio del derecho a la reparación. A tal fin, el juez podrá:

a) ordenar la divulgación bajo procedimiento in camera, restringiendo el acceso a la información técnica al juez, los peritos designados y los letrados de las partes, bajo compromiso escrito de confidencialidad;

b) designar peritos técnicos con acceso restringido que examinen la documentación y emitan dictamen sin revelar el detalle del código fuente o los algoritmos propietarios, limitándose a informar sobre la existencia o ausencia de defectos, sesgos o incumplimientos relevantes para la causa;

c) establecer que la información obtenida bajo procedimiento in camera no podrá ser utilizada para fines distintos del proceso judicial en curso.

La filtración, divulgación o uso indebido de información obtenida bajo este procedimiento constituirá falta grave sancionable conforme la legislación procesal aplicable, sin perjuicio de la responsabilidad civil y penal que corresponda.

La negativa injustificada del operador a divulgar la información ordenada judicialmente generará una presunción de causalidad a favor de la persona afectada.

ARTÍCULO 10 — *Tipos de daño indemnizable.* Son daños indemnizables bajo la presente ley:

a) Daño emergente y lucro cesante.

b) Daño moral, incluyendo el sufrimiento, la angustia, la pérdida de oportunidades vitales y la afectación de la dignidad.

c) Daño a la integridad mental y la continuidad psicológica, cuando el sistema involucre neurotecnologías o procesamiento de neurodatos.

d) Daño derivado de discriminación algorítmica, incluyendo la pérdida de oportunidades de empleo, crédito, educación, vivienda o servicios esenciales por decisión sesgada del sistema.

e) Daño a datos personales, incluyendo la destrucción, pérdida, alteración o exposición no autorizada.

f) Pérdida de autonomía decisoria, cuando el sistema haya condicionado, manipulado o sustituido indebidamente la capacidad de decisión del afectado.

g) Daño al proyecto de vida, cuando el sistema haya causado una alteración grave y duradera de las condiciones de existencia de la persona afectada.

La enumeración precedente no es taxativa. Todo daño jurídicamente relevante causado por un sistema de IA será indemnizable conforme los principios generales de la responsabilidad civil.

ARTÍCULO 11 — *Daños punitivos.* Cuando el daño causado por un sistema de IA resulte de una conducta dolosa, gravemente culposa o de manifiesta indiferencia hacia los derechos de la persona afectada, el juez podrá aplicar una multa civil a favor del afectado de hasta cinco (5) veces el monto de la indemnización compensatoria. Se considerará especialmente la ocultación deliberada de defectos conocidos, la omisión dolosa de medidas correctivas, la comercialización del sistema con conocimiento de sus riesgos sin informar a los usuarios, y el beneficio económico obtenido por el operador como consecuencia de la conducta dañosa.

ARTÍCULO 12 — *Seguro obligatorio y pricing regulatorio del riesgo.* Los proveedores e implementadores de sistemas de IA de alto riesgo deberán contratar un seguro de responsabilidad civil que cubra los daños previstos en la presente ley, por montos mínimos que establecerá la reglamentación conforme la categoría de riesgo del sistema.

La falta de contratación del seguro obligatorio constituirá infracción grave y no eximirá al operador de su responsabilidad personal e ilimitada.

La Autoridad de Aplicación, en coordinación con la Superintendencia de Seguros de la Nación, establecerá las condiciones mínimas de las pólizas, los montos de cobertura según categorías de riesgo y los mecanismos de actualización. A tal fin, implementará un sistema de pricing regulatorio del riesgo basado en los siguientes criterios:

a) Diferenciación tarifaria por nivel de riesgo: los sistemas clasificados en las categorías de mayor riesgo del Anexo I abonarán primas proporcionalmente superiores a las de los sistemas de menor riesgo dentro del mismo anexo. La Autoridad de Aplicación establecerá bandas tarifarias mínimas y máximas para cada categoría;

b) Reducción automática por cumplimiento certificado: los operadores que acrediten haber obtenido certificaciones de conformidad reconocidas por la Autoridad de Aplicación, realizado auditorías algorítmicas periódicas por auditores certificados, e implementado programas de gestión de riesgos conforme estándares internacionales, accederán a una reducción de la prima base de hasta un treinta por ciento (30%);

c) Recargo por siniestralidad: los operadores cuyos sistemas registren incidentes de daño reportados a la Autoridad de Aplicación estarán sujetos a recargos progresivos sobre la prima base, conforme la escala que establezca la reglamentación;

d) Bonificación por transparencia: los operadores que voluntariamente publiquen evaluaciones de impacto algorítmico, sometan sus sistemas a auditorías abiertas o implementen mecanismos de explicabilidad que excedan los requisitos mínimos legales, podrán acceder a una bonificación adicional de hasta un quince por ciento (15%) sobre la prima resultante.

Cuando el mercado asegurador no ofrezca cobertura adecuada para determinadas categorías de sistemas de IA de alto riesgo, la Autoridad de Aplicación, en coordinación con la Superintendencia de Seguros de la Nación y el Ministerio de Economía, promoverá la creación de:

a) fondos de garantía sectoriales, constituidos mediante aportes obligatorios de

los operadores de cada sector, que operarán como cobertura subsidiaria cuando la indemnización exceda los límites de la póliza individual;

b) esquemas de coaseguro obligatorio o pool de riesgo entre aseguradoras, para distribuir el riesgo de siniestros de IA de alta cuantía;

c) mecanismos de reaseguro internacional, que permitan transferir parcialmente el riesgo a mercados con mayor capacidad de absorción.

La reglamentación establecerá los plazos y condiciones para la constitución de estos mecanismos. La Autoridad de Aplicación publicará anualmente un informe de siniestralidad y tarifación que servirá como base técnica para la actualización de las bandas tarifarias.

ARTÍCULO 13 — *Prescripción.* Las acciones de responsabilidad civil previstas en la presente ley prescribirán a los tres (3) años contados desde que la persona afectada tuvo conocimiento o debió razonablemente tener conocimiento del daño y de la identidad del operador responsable.

En ningún caso la acción podrá ejercerse transcurridos diez (10) años desde la fecha en que el sistema de IA fue puesto en servicio, salvo para daños a la salud o la integridad física o mental, en cuyo caso el plazo máximo será de veinte (20) años.

TÍTULO III — DEBERES DE DILIGENCIA Y TRANSPARENCIA

ARTÍCULO 14 — *Deberes generales del proveedor.* El proveedor de un sistema de IA deberá:

a) Diseñar, desarrollar y probar el sistema siguiendo el estado del arte y las normas técnicas aplicables, identificando, evaluando y mitigando los riesgos previsibles.

b) Proporcionar instrucciones claras y completas sobre la finalidad prevista del sistema, sus capacidades, limitaciones, riesgos conocidos y medidas de supervisión humana requeridas.

c) Mantener la documentación técnica y los registros de funcionamiento por un período mínimo de diez (10) años desde la puesta en servicio del sistema o el período que establezca la legislación sectorial aplicable.

d) Implementar un sistema de monitoreo post-mercado que permita identificar riesgos emergentes y adoptar medidas correctivas.

e) Informar a los implementadores y a la Autoridad de Aplicación sobre defectos o riesgos descubiertos tras la puesta en servicio.

f) Cuando se trate de sistemas de IA de alto riesgo, realizar evaluaciones de conformidad y mantener un sistema de gestión de calidad conforme las normas que establezca la Autoridad de Aplicación.

ARTÍCULO 15 — *Deberes generales del implementador.* El implementador de un sistema de IA deberá:

a) Utilizar el sistema conforme a las instrucciones del proveedor y su finalidad prevista.

b) Asegurar la supervisión humana efectiva del sistema, designando personas competentes con autoridad para intervenir, corregir o detener su funcionamiento.

c) Informar a las personas afectadas por las decisiones del sistema sobre la utilización de IA, salvo que resulte evidente por las circunstancias.

d) Suspender el uso del sistema y notificar al proveedor y a la Autoridad de Aplicación cuando detecte riesgos para la seguridad o los derechos de las personas.

e) Mantener registros de uso del sistema por un período mínimo de cinco (5) años.

ARTÍCULO 16 — *Deber de transparencia al afectado.* Toda persona que sea objeto de una decisión adoptada o asistida por un sistema de IA que produzca efectos jurídicos o la afecte significativamente, tendrá derecho a:

a) Ser informada de que la decisión fue adoptada o asistida por un sistema de IA.

b) Obtener una explicación comprensible de los principales factores y la lógica general que condujeron al resultado específico.

c) Conocer los datos de entrada que fueron determinantes para el resultado.

d) Impugnar la decisión y solicitar la intervención de una persona humana competente para su revisión.

El cumplimiento de este deber no podrá ser sustituido por la mera referencia a la complejidad técnica del sistema.

ARTÍCULO 16 bis — *Mediación técnica previa optativa.* Antes de iniciar una acción

judicial por daños causados por un sistema de IA, las partes podrán someter la controversia a un procedimiento de mediación técnica especializada ante mediadores inscriptos en un registro específico que la Autoridad de Aplicación creará y mantendrá actualizado, integrado por profesionales con formación acreditada en inteligencia artificial y en resolución alternativa de disputas.

El procedimiento de mediación técnica se regirá por las siguientes reglas:

a) Carácter optativo: la mediación técnica no será requisito de admisibilidad de la acción judicial. Cualquiera de las partes podrá solicitarla, pero no será obligatoria para la contraparte, salvo que ambas partes consientan participar;

b) Plazo: el procedimiento no podrá exceder los sesenta (60) días corridos desde la aceptación de ambas partes, prorrogable por treinta (30) días adicionales por acuerdo;

c) Asistencia pericial: el mediador podrá solicitar a la UTIARA un informe técnico preliminar no vinculante sobre las cuestiones en disputa, que deberá ser emitido dentro de los veinte (20) días;

d) Confidencialidad: las actuaciones, declaraciones y documentos producidos durante la mediación serán confidenciales y no podrán ser utilizados como prueba en un eventual proceso judicial posterior;

e) Efecto sobre la prescripción: la solicitud de mediación técnica suspenderá el curso de la prescripción de la acción judicial por el plazo de duración del procedimiento;

f) Acuerdo homologable: el acuerdo alcanzado en mediación técnica podrá ser sometido a homologación judicial, adquiriendo los efectos de cosa juzgada.

La Autoridad de Aplicación establecerá un régimen de aranceles reducidos para la mediación técnica, pudiendo establecer la gratuidad del servicio para personas humanas cuando la cuantía del reclamo no supere el equivalente a cincuenta (50) salarios mínimos vitales y móviles. Los costos del informe técnico de la UTIARA serán soportados por las partes en partes iguales, salvo acuerdo en contrario.

TÍTULO IV — ACCIONES JUDICIALES

ARTÍCULO 17 — *Competencia.* Será competente el juez del domicilio de la persona afectada, el del lugar del hecho dañoso, o el del domicilio del operador, a elección del actor. Procederá el fuero federal cuando el sistema de IA sea operado por organismos públicos nacionales, cuando los efectos del daño se extiendan a más de una jurisdicción

provincial, o cuando el operador esté domiciliado en el extranjero.

ARTÍCULO 18 — *Medidas cautelares.* El juez podrá ordenar, a pedido de la persona afectada o de oficio, medidas cautelares tales como:

a) la suspensión del funcionamiento del sistema de IA o de una funcionalidad específica;

b) la preservación de los registros de funcionamiento y la documentación técnica;

c) la prohibición de destruir, alterar u ocultar información relevante;

d) cualquier otra medida que resulte necesaria para prevenir la agravación del daño o garantizar la efectividad de la sentencia.

ARTÍCULO 19 — *Acciones colectivas.* Será procedente la acción colectiva cuando una pluralidad de personas haya sido afectada por el mismo sistema de IA o por un patrón sistémico de funcionamiento dañoso.

Tendrán legitimación activa: el Defensor del Pueblo, las asociaciones de defensa de consumidores registradas, la Autoridad de Aplicación y los afectados directos.

El tribunal podrá establecer procedimientos simplificados para la determinación y liquidación de daños individuales dentro de la acción colectiva. Los honorarios de los letrados de la parte actora podrán fijarse con base en el beneficio obtenido para la clase.

ARTÍCULO 20 — *Pericia técnica y asistencia judicial especializada.* En todo proceso en que se debata la responsabilidad por daños de un sistema de IA, el juez podrá designar de oficio peritos técnicos especializados en inteligencia artificial, cuya designación se realizará de un registro de peritos que la Autoridad de Aplicación elaborará y mantendrá actualizado. Los costos de la pericia serán soportados por la parte vencida, salvo que el juez disponga su distribución equitativa atendiendo a las circunstancias del caso.

Cuando la complejidad técnica del caso lo requiera, el juez podrá solicitar a la UTIARA la emisión de un dictamen pericial institucional, que tendrá el carácter de prueba pericial oficial y deberá ser producido dentro de los sesenta (60) días de requerido. La UTIARA no podrá negarse a emitir el dictamen solicitado.

ARTÍCULO 20 bis — *Capacitación judicial obligatoria y asistencia técnica permanente.* El Consejo de la Magistratura de la Nación y los consejos de la magistratura provinciales, en coordinación con la Autoridad de Aplicación, implementarán programas de capacitación obligatoria y continua para jueces, secretarios y funcionarios judiciales en materia de inteligencia artificial, responsabilidad algorítmica y valoración de prueba

técnica, dentro de los doce (12) meses de la entrada en vigencia de la presente ley.

La Autoridad de Aplicación mantendrá un servicio de asistencia técnica permanente al Poder Judicial, al que los jueces podrán recurrir para obtener orientación preliminar sobre cuestiones técnicas vinculadas a sistemas de IA, sin que dicha asistencia sustituya la prueba pericial ni vincule al magistrado.

Invítase a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a los programas de capacitación judicial previstos en este artículo y a implementar mecanismos análogos en sus respectivas jurisdicciones.

TÍTULO V — AUTORIDAD DE APLICACIÓN Y REGISTRO

ARTÍCULO 21 — ***Autoridad de Aplicación.*** Será Autoridad de Aplicación de la presente ley el organismo nacional con competencia en materia de protección de datos personales, el cual ejercerá sus funciones en coordinación con la Secretaría de Innovación, Ciencia y Tecnología o el organismo que la reemplace.

Créase dentro de la Autoridad de Aplicación la Unidad Técnica de Inteligencia Artificial y Responsabilidad Algorítmica (UTIARA) como órgano especializado con autonomía técnica y funcional, integrado por profesionales en inteligencia artificial, ingeniería de software, ciencia de datos, neurociencia computacional y derecho tecnológico.

La UTIARA se regirá por las siguientes garantías de independencia institucional:

a) Mandato fijo: el Director o Directora de la UTIARA será designado por un mandato de cinco (5) años, renovable por una única vez, y solo podrá ser removido por causas graves debidamente fundadas y previo procedimiento que garantice el derecho de defensa;

b) Designación con intervención del Honorable Senado de la Nación: el Director o Directora será propuesto por el titular de la Autoridad de Aplicación y designado previa audiencia pública ante la Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión del Honorable Senado de la Nación, o la comisión que la reemplace, la cual podrá formular objeciones fundadas dentro de los treinta (30) días. En caso de objeción, el titular de la Autoridad de Aplicación deberá proponer un nuevo candidato;

c) Presupuesto protegido: la UTIARA contará con una asignación presupuestaria específica dentro del presupuesto de la Autoridad de Aplicación, que no podrá ser inferior al equivalente al cero coma dos por ciento (0,2%) de la recaudación anual en concepto de tasas de registro de sistemas de IA de alto riesgo y multas

aplicadas conforme la presente ley. El Poder Ejecutivo Nacional no podrá disponer la reasignación, reducción o indisponibilidad de los créditos presupuestarios asignados a la UTIARA sin autorización legislativa;

d) Incompatibilidades: el Director o Directora y los profesionales de planta de la UTIARA no podrán mantener vínculos laborales, contractuales, societarios o de consultoría con operadores de sistemas de IA sujetos a la presente ley durante su mandato y hasta dos (2) años después de su cese.

La UTIARA será responsable de:

a) la evaluación técnica de incidentes de daños por IA;

b) la clasificación de sistemas por nivel de riesgo;

c) la certificación de auditores algorítmicos;

d) la asistencia técnica al Poder Judicial mediante dictámenes periciales institucionales;

e) el mantenimiento del registro de peritos especializados;

f) la elaboración de estándares técnicos y guías de buenas prácticas;

g) la administración del sistema de pricing regulatorio del riesgo previsto en el artículo 12.

La UTIARA podrá convocar a especialistas del CONICET, universidades nacionales y organismos técnicos internacionales como asesores ad hoc.

ARTÍCULO 22 — ***Registro Nacional de Sistemas de IA de Alto Riesgo.*** Créase el Registro Nacional de Sistemas de Inteligencia Artificial de Alto Riesgo en el ámbito de la Autoridad de Aplicación. Todo proveedor de un sistema de IA de alto riesgo que lo introduzca en el mercado argentino deberá inscribirlo, informando:

a) Datos del proveedor y del sistema.

b) Descripción de la finalidad, capacidades, limitaciones y riesgos conocidos.

c) Documentación de las evaluaciones de riesgo y conformidad realizadas.

d) Información sobre el seguro de responsabilidad civil contratado.

e) Instrucciones de uso y medidas de supervisión humana requeridas.

El Registro será de acceso público en su información no confidencial.

ARTÍCULO 23 — *Facultades de la Autoridad.* La Autoridad de Aplicación tendrá las siguientes facultades específicas:

a) Administrar el Registro Nacional.

b) Clasificar sistemas de IA por nivel de riesgo y actualizar la clasificación con periodicidad bienal.

c) Investigar incidentes de daños causados por sistemas de IA, de oficio o por denuncia.

d) Emitir recomendaciones sobre estándares de seguridad y deberes de diligencia.

e) Mantener el registro de peritos técnicos especializados.

f) Establecer los montos mínimos de seguro obligatorio y administrar el sistema de pricing regulatorio del riesgo.

g) Publicar informes periódicos sobre siniestralidad de sistemas de IA.

h) Cooperar con autoridades de otros países en materia de responsabilidad por IA.

i) Promover el reconocimiento internacional del régimen de responsabilidad civil por IA argentino como estándar regional de referencia, mediante acuerdos bilaterales, participación en foros multilaterales y mecanismos de equivalencia regulatoria.

ARTÍCULO 23 bis — *Índice Nacional de Confiabilidad de Sistemas de IA (INCONFIA).* Créase el Índice Nacional de Confiabilidad de Sistemas de Inteligencia Artificial (INCONFIA) como instrumento público de evaluación y transparencia, administrado por la UTIARA. El INCONFIA asignará a cada sistema de IA de alto riesgo inscripto en el Registro Nacional una calificación de confiabilidad basada en los siguientes criterios ponderados:

a) Historial de siniestralidad: frecuencia y gravedad de los incidentes de daño reportados o investigados por la Autoridad de Aplicación;

b) Grado de cumplimiento normativo: resultado de las auditorías algorítmicas, evaluaciones de conformidad y cumplimiento de los deberes de diligencia y transparencia;

c) Nivel de transparencia: existencia y calidad de mecanismos de explicabilidad,

publicación voluntaria de evaluaciones de impacto algorítmico y cooperación con la Autoridad de Aplicación;

d) Certificaciones obtenidas: certificaciones de conformidad nacionales e internacionales reconocidas por la Autoridad de Aplicación.

El INCONFIA será de acceso público y se actualizará con periodicidad semestral. La calificación se expresará mediante una escala estandarizada que la reglamentación determinará, y deberá ser exhibida por los operadores en toda comunicación comercial, interfaz de usuario y documentación contractual de sistemas de IA de alto riesgo.

La calificación del INCONFIA no constituirá por sí sola prueba de diligencia ni de negligencia en sede judicial, pero podrá ser valorada como indicio por el juez. Los operadores que obtengan las calificaciones más altas podrán acceder a las bonificaciones previstas en el sistema de pricing regulatorio del riesgo del artículo 12.

TÍTULO VI — SANDBOX DE RESPONSABILIDAD

ARTÍCULO 24 — *Sandbox de responsabilidad.* La Autoridad de Aplicación podrá establecer un régimen de sandbox de responsabilidad que permita probar sistemas de IA innovadores bajo condiciones controladas, con las siguientes características:

a) Duración de hasta veinticuatro (24) meses, prorrogable por una vez.

b) Cobertura de seguro específica para el período de prueba.

c) Supervisión continua de la Autoridad de Aplicación.

d) Consentimiento informado reforzado de las personas que interactúen con el sistema.

e) Publicación de los resultados y aprendizajes para la mejora regulatoria.

f) Exención parcial de la obligación de registro, sin afectar la responsabilidad civil por daños efectivos.

La participación en el sandbox no exime de responsabilidad por daños causados pero podrá ser considerada como circunstancia atenuante en la graduación de daños punitivos.

TÍTULO VII — COORDINACIÓN NORMATIVA Y DISPOSICIONES FINALES

ARTÍCULO 25 — *Coordinación con otras normas.* La presente ley se aplicará de manera

complementaria y coordinada con la normativa vigente en materia de protección de datos personales, neuroderechos, soberanía cognitiva y protección de la atención humana, la Ley Nº 24.240 de Defensa del Consumidor, el Código Civil y Comercial de la Nación y toda otra legislación aplicable. En caso de conflicto, prevalecerá la norma que otorgue mayor protección a la persona afectada. Se presumirá la existencia de relación de consumo en los términos de la Ley Nº 24.240 cuando el sistema de IA sea ofrecido al público a través de plataformas digitales, aplicaciones móviles, servicios de tecnología financiera (fintech), asistentes virtuales o cualquier otra interfaz dirigida a usuarios finales, resultando aplicables las normas de defensa del consumidor en forma concurrente con las disposiciones de la presente ley.

ARTÍCULO 26 — *Cláusula pro-innovación.* La interpretación de la presente ley favorecerá el desarrollo de la inteligencia artificial responsable en la Argentina. El régimen de responsabilidad no deberá imponer cargas desproporcionadas que desincentiven la investigación científica, el emprendimiento tecnológico o la competitividad de la economía digital, siempre que no se menoscabe la reparación efectiva de los daños ni los derechos fundamentales de las personas.

ARTÍCULO 27 — *Plazo de adecuación escalonado.* Los operadores de sistemas de IA de alto riesgo que al momento de la entrada en vigencia se encuentren operando en el mercado argentino deberán cumplir las obligaciones de registro y seguro obligatorio conforme el siguiente cronograma escalonado por sector:

a) Sistemas de atención sanitaria (Anexo I, categoría I) y neurotecnologías (Anexo I, categoría IX): seis (6) meses desde la entrada en vigencia;

b) Sistemas de infraestructura crítica (Anexo I, categoría III), administración de justicia y seguridad (Anexo I, categoría VI) y riesgo sistémico financiero (Anexo I, categoría XI): doce (12) meses desde la entrada en vigencia;

c) Sistemas de evaluación crediticia y seguros (Anexo I, categoría IV), empleo (Anexo I, categoría V), educación (Anexo I, categoría VII) y servicios públicos esenciales (Anexo I, categoría VIII): dieciocho (18) meses desde la entrada en vigencia;

d) Sistemas de transporte (Anexo I, categoría II), biometría (Anexo I, categoría X) y riesgo sistémico informativo y electoral (Anexo I, categoría XII): dieciocho (18) meses desde la entrada en vigencia.

Los proveedores que califiquen como micro, pequeñas o medianas empresas conforme la normativa vigente de la Secretaría de Industria y Desarrollo Productivo dispondrán de un plazo adicional de seis (6) meses sobre los plazos establecidos en los incisos

precedentes para cumplir con la obligación de seguro obligatorio, sin perjuicio de su obligación de registro.

La obligación de responder por los daños causados rige desde la entrada en vigencia de la presente ley, con independencia de los plazos de adecuación.

ARTÍCULO 28 — *Revisión tecnológica.* La presente ley será objeto de revisión integral a los cuatro (4) años de su entrada en vigencia, con informe de la Autoridad de Aplicación al Congreso de la Nación, a los efectos de evaluar su adecuación al estado del arte y la efectividad del régimen.

ARTÍCULO 29 — *Cláusula transitoria — Autoridad de Aplicación interina.* Hasta tanto se constituya o designe formalmente el organismo nacional con competencia en materia de protección de datos personales con las facultades previstas en la presente ley, ejercerá transitoriamente las funciones de Autoridad de Aplicación la Agencia de Acceso a la Información Pública (AAIP) o el organismo que la suceda en sus competencias, con el apoyo técnico de la Secretaría de Innovación, Ciencia y Tecnología. La designación del primer Director o Directora de la UTIARA deberá realizarse dentro de los ciento ochenta (180) días de la entrada en vigencia de la presente ley.

ARTÍCULO 30 — *Reglamentación.* El Poder Ejecutivo Nacional reglamentará la presente ley dentro de los ciento ochenta (180) días de su publicación.

ARTÍCULO 31 — *Vigencia.* La presente ley entrará en vigencia a los noventa (90) días de su publicación.

ARTÍCULO 32 — *Comuníquese al Poder Ejecutivo Nacional.*

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN

ANEXO I

CATEGORÍAS DE SISTEMAS DE INTELIGENCIA ARTIFICIAL DE ALTO RIESGO

(Artículo 3º, inciso b)

I. Atención sanitaria: sistemas de IA utilizados para diagnóstico médico, triaje, prescripción de tratamientos o asignación de recursos sanitarios.

II. Transporte: sistemas de conducción autónoma o asistencia a la conducción con control parcial o total del vehículo.

III. Infraestructura crítica: sistemas que gestionan redes de energía, agua, telecomunicaciones o transporte público.

IV. Evaluación crediticia y seguros: sistemas que determinan acceso a crédito, scoring crediticio, fijación de primas o cobertura de seguros.

V. Empleo: sistemas utilizados para selección, contratación, evaluación de desempeño, promoción o despido de trabajadores.

VI. Administración de justicia y seguridad: sistemas que asisten en la determinación de penas, evaluación de riesgo de reincidencia, investigación penal o vigilancia.

VII. Educación: sistemas que determinan acceso, evaluación o acreditación educativa.

VIII. Servicios públicos esenciales: sistemas que determinan acceso a prestaciones sociales, vivienda o servicios públicos.

IX. Neurotecnologías: sistemas que procesan neurodatos o interactúan con el sistema nervioso.

X. Biometría: sistemas de identificación biométrica remota o categorización biométrica.

XI. Riesgo sistémico financiero: sistemas de IA cuyo funcionamiento o falla pueda producir efectos en cascada sobre mercados financieros, sistemas de pagos o estabilidad económica, incluyendo trading algorítmico de alta frecuencia y sistemas de gestión de riesgo sistémico.

XII. Riesgo sistémico informativo y electoral: sistemas de IA que, por su escala de

distribución, puedan alterar significativamente la formación de la opinión pública, los procesos electorales o el debate democrático, incluyendo sistemas de recomendación de contenidos de alcance masivo y sistemas de generación o manipulación de contenidos sintéticos (deepfakes) con potencial de difusión masiva.

DIPUTADOS
ARGENTINA

FUNDAMENTOS

Señor Presidente:

I. El vacío regulatorio global. En febrero de 2025, la Comisión Europea retiró la propuesta de AI Liability Directive, dejando sin resolver el régimen de responsabilidad civil por daños de IA en la jurisdicción que más ha avanzado en su regulación. Posteriormente, el Parlamento Europeo publicó un estudio que recomienda crear un régimen de responsabilidad estricta para sistemas de alto riesgo, reconociendo que ni el AI Act ni la Directiva de Responsabilidad por Productos son suficientes. En Estados Unidos, la regulación permanece fragmentada entre estados sin un marco federal unificado. En China, el enfoque es estatal y administrativo, sin un régimen de responsabilidad civil autónomo. El resultado: existe un vacío regulatorio global que la Argentina puede llenar, posicionándose como la primera jurisdicción del mundo con un régimen integral de responsabilidad civil por daños de IA.

II. La necesidad argentina. El Código Civil y Comercial de la Nación no contempla las particularidades de los sistemas de IA: su complejidad, opacidad, autonomía y capacidad de autoevolución hacen que las reglas generales de responsabilidad por culpa resulten inadecuadas. La víctima de un daño causado por IA enfrenta una asimetría informativa radical: no puede demostrar el defecto del sistema porque no tiene acceso a la documentación técnica, los datos de entrenamiento ni los registros de funcionamiento. Esta asimetría, denominada “efecto caja negra”, exige un régimen específico que invierta o facilite la carga de la prueba.

III. Arquitectura del proyecto. El proyecto adopta un sistema dual de responsabilidad inspirado en la mejor doctrina comparada: responsabilidad objetiva para sistemas de alto riesgo (arts. 4-6) y responsabilidad subjetiva con presunción de causalidad para el resto (arts. 7-8). Esta distinción es coherente con la clasificación por niveles de riesgo del AI Act europeo y con las mejores prácticas internacionales en materia de protección de datos personales.

El proyecto introduce nueve mecanismos innovadores que lo distinguen de los antecedentes comparados. Primero, el derecho de acceso a la información del sistema (art. 9), que permite a la víctima obtener judicialmente la documentación técnica

necesaria para evaluar y sustentar su reclamo, con protección del secreto industrial pero sin que éste pueda impedir la reparación. La negativa injustificada genera presunción de causalidad. Segundo, la inversión de la carga probatoria por opacidad (art. 8 bis), que cuando concurren daño, sistema de alto riesgo y opacidad del sistema, traslada al operador la obligación de probar su diligencia plena, resolviendo el problema del "efecto caja negra" en sede judicial. Tercero, un catálogo ampliado de daños indemnizables (art. 10) que incluye discriminación algorítmica, pérdida de autonomía decisoria, daño a la integridad mental y daño al proyecto de vida, categorías inexistentes en la legislación actual. Cuarto, el seguro obligatorio con pricing dinámico del riesgo (art. 12), que no solo socializa el costo del riesgo y garantiza la solvencia del responsable, sino que convierte la regulación en un motor de mercado mediante incentivos tarifarios que premian el cumplimiento y penalizan la siniestralidad. Quinto, el sandbox de responsabilidad (art. 24), que permite probar sistemas innovadores bajo supervisión sin eximir de responsabilidad por daños efectivos. Sexto, el blindaje institucional de la UTIARA (art. 21), que asegura la independencia técnica de la autoridad especializada mediante mandato fijo, designación con intervención del Senado, presupuesto protegido e incompatibilidades estrictas. Séptimo, la mediación técnica especializada (art. 16 bis), que ofrece una vía de resolución alternativa de disputas con peritos certificados, reduciendo la litigiosidad sin sacrificar el acceso a la justicia. Octavo, el régimen transitorio escalonado por sector (art. 27), que calibra los plazos de adecuación según la criticidad de cada sector y contempla plazos extendidos para PyMEs. Noveno, el Índice Nacional de Confiabilidad de Sistemas de IA (INCONFIA, art. 23 bis), un scoring público de los sistemas de IA de alto riesgo basado en siniestralidad, cumplimiento normativo, transparencia y certificaciones, que introduce un efecto reputacional de mercado y vincula la calificación con el pricing regulatorio del riesgo.

IV. Equilibrio innovación-protección. El proyecto incluye una cláusula pro-innovación explícita (art. 26) y un sandbox regulatorio (art. 24). La responsabilidad objetiva se limita a sistemas de alto riesgo; el resto opera bajo culpa con presunción de causalidad. Los deberes de diligencia se calibran según el nivel de riesgo. El seguro obligatorio socializa el costo y brinda previsibilidad a los operadores, mientras que el pricing dinámico del riesgo convierte la ley en un incentivo de mercado para la calidad y la transparencia. Este diseño busca que la regulación sea un motor de innovación responsable y no un freno a la competitividad.

V. Enforcement técnico. El proyecto reconoce que la efectividad del régimen depende de la capacidad técnica del sistema judicial para comprender y valorar las pruebas

vinculadas a sistemas de IA. Por ello, establece tres mecanismos complementarios: el registro de peritos especializados administrado por la UTIARA (art. 20), el dictamen pericial institucional obligatorio de la UTIARA a solicitud judicial (art. 20), y los programas de capacitación judicial obligatoria en materia de inteligencia artificial (art. 20 bis). Este trípode garantiza que los jueces cuenten con los instrumentos técnicos necesarios para resolver las controversias con solvencia, reduciendo el riesgo de que la sofisticación tecnológica opere como barrera de acceso a la justicia.

VI. Integración sistémica. Este proyecto completa el ecosistema legislativo en materia de gobernanza de inteligencia artificial, complementando la normativa vigente y los proyectos en trámite en materia de neuroderechos, soberanía cognitiva y protección integral de datos personales. La Autoridad de Aplicación se designa en el organismo nacional competente en materia de protección de datos personales, lo que evita la proliferación de organismos y asegura coherencia regulatoria. La coordinación normativa (art. 25) establece la prevalencia de la norma más protectora. A su vez, se prevé una cláusula transitoria (art. 29) para garantizar la operatividad inmediata de la ley.

VII. Posicionamiento geopolítico. Con esta ley, la Argentina sería la primera jurisdicción del mundo en contar con un régimen completo e integrado de responsabilidad civil por daños de IA, en un momento en que la Unión Europea retrocedió en su propia propuesta, Estados Unidos carece de marco federal y China opera bajo un modelo estatal incompatible con la tradición civilista. La cláusula de extraterritorialidad (art. 2, inc. d), reforzada con el criterio de volumen significativo de mercado para cerrar el riesgo de forum shopping inverso, y la facultad de la Autoridad de Aplicación de promover el reconocimiento internacional del régimen argentino (art. 23, inc. i) posicionan al país como hub regulatorio de referencia y como potencial exportador de estándares normativos para la región y el mundo. Esto fortalece la confianza necesaria para la adopción responsable de la inteligencia artificial y proyecta a la Argentina como líder en gobernanza tecnológica responsable.

VIII. La ley como infraestructura de mercado. Este proyecto no es una regulación estática sino una infraestructura jurídica para la economía de la inteligencia artificial. Regula simultáneamente cuatro flujos esenciales: el flujo de información (mediante los deberes de transparencia y el derecho de acceso probatorio), el flujo de riesgo (mediante el seguro obligatorio con pricing dinámico), el flujo de responsabilidad

(mediante el sistema dual de causalidad y la inversión de carga probatoria) y el flujo de confianza (mediante el INCONFIA, las certificaciones y la reparación efectiva). La mediación técnica especializada reduce los costos de transacción del sistema. El régimen transitorio escalonado evita disrupciones sectoriales. El resultado es un marco que incentiva la calidad, premia la transparencia, socializa el riesgo y garantiza la reparación, convirtiendo la regulación en un activo competitivo para la Argentina.

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

LIC. MARCELA MARINA PAGANO

DIPUTADA DE LA NACIÓN