rrp/mrb/com
S.79ª/373ª

Oficio Nº 20.843

VALPARAÍSO, 13 de octubre de 2025

A S.E. EL
PRESIDENTE DEL
H. SENADO

Tengo a honra comunicar a Vuestra Excelencia que, con motivo de la moción, el mensaje, informes y demás antecedentes que tengo a honra pasar a manos de V.E., la Cámara de Diputados ha aprobado el siguiente proyecto de ley, que regula los sistemas de inteligencia artificial, correspondiente a los boletines Nos 15.869-19 y 16.821-19, refundidos:

PROYECTO DE LEY

"TÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Objeto de la ley. Esta ley tiene por objeto regular los usos de los sistemas de Inteligencia Artificial (en adelante IA), promover su creación, desarrollo, innovación e implementación, y proporcionar un marco normativo que vele por el desarrollo sostenible y ético de la IA al servicio de las personas, respetuoso de los principios democráticos y del estado de derecho.

El Estado de Chile, por medio de sus instituciones, promoverá el uso, desarrollo de la IA y su infraestructura necesaria, velará por el

cumplimiento del marco institucional y normativo bajo el cual se organiza la República de Chile, con respeto de los derechos fundamentales de las personas consagrados en la Constitución Política de la República, y promoverá la igualdad de derechos a fin de eliminar toda forma de discriminación arbitraria.

Artículo 2.- Ámbito de aplicación. Esta ley será aplicable a:

1. Los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en el territorio nacional.

2. Los implementadores de sistemas de IA que se encuentren domiciliados en el territorio nacional.

3. Los proveedores e implementadores de sistemas de IA que se encuentren domiciliados en el extranjero, cuando la información de salida generada por el sistema de IA se utilice en Chile.

4. Los importadores y distribuidores de sistemas de IA, así como a los representantes autorizados de los proveedores de sistemas de IA, cuando dichos importadores, distribuidores y representantes autorizados se encuentren domiciliados en el territorio nacional.

Con todo, esta ley no será aplicable a:

a) Los sistemas de IA desarrollados y utilizados con fines de defensa nacional. Una resolución reservada expedida por el Ministerio de Defensa Nacional identificará y listará los sistemas de IA que quedan comprendidos dentro de la presente excepción.

Para dar cumplimiento a lo anterior, el Ministerio de Defensa Nacional dictará un reglamento con los criterios que permitan identificar y listar los sistemas de IA mencionados en el párrafo precedente.

b) Las actividades de investigación, pruebas y desarrollo de sistemas de IA de forma previa a su introducción en el mercado o puesta en servicio, siempre que dichas actividades se lleven a cabo con respeto de los derechos fundamentales de las personas. Si se producen daños con ocasión de dichas actividades se responderá de conformidad con los artículos 12 y 18.

Las pruebas en condiciones reales no estarán cubiertas por esta exención.

———c) Componentes de IA proporcionados en el marco de licencias libres y de código abierto, salvo que sean comercializados o puestos en servicio por un proveedor como parte de un sistema de IA de alto riesgo. Si se producen daños con ocasión de este tipo de desarrollos se responderá de acuerdo con lo dispuesto en el artículo 19.

Artículo 3.- Definiciones. Para los efectos

de esta ley, se entenderá por:

1. Sistema de IA: sistema basado en máquinas, algoritmos o modelos matemáticos que, en función de objetivos explícitos o implícitos infiere, a partir de los datos de entrada que recibe, cómo generar resultados o salidas, tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos sociales, físicos o virtuales. Los distintos sistemas de IA pueden variar en sus niveles de autonomía y adaptabilidad tras su implementación.

2. Sistema de IA de uso general: aquel capaz de realizar múltiples funciones de aplicación general a la vez, tales como el reconocimiento de imágenes o voz, procesamiento de audio, generación de video, detección de patrones, respuesta a preguntas, traducción, entre otros, y que puede proporcionar resultados o salidas tanto previsibles como no previsibles.

3. Riesgo: la combinación de la probabilidad de que se produzca un daño a las personas, a su salud, a su seguridad o a sus derechos fundamentales y la gravedad de dicho daño.

4. Riesgo significativo: riesgo resultante de la combinación de su gravedad, intensidad, probabilidad de ocurrencia y duración de sus efectos y su capacidad de afectar a una o varias personas naturales.

5. Proveedor: la persona natural o

jurídica u organismo del Estado que desarrolla un sistema de IA con miras a introducirlo en el mercado o ponerlo en servicio, a título gratuito u oneroso.

6. Implementador: la persona natural o jurídica u organismo del Estado que utiliza un sistema de IA, salvo que se trate de su uso privado, en los términos de la ley N° 17.336, sobre propiedad intelectual.

7. Representante autorizado: la persona natural o jurídica domiciliada en Chile que recibe y acepta el mandato por escrito de un proveedor de un sistema de IA para cumplir con las obligaciones establecidas en esta ley en representación de dicho proveedor.

8. Importador: la persona natural o jurídica domiciliada en Chile que introduce en el mercado o pone en servicio un sistema de IA que lleve el nombre o la marca comercial de una persona natural o jurídica establecida fuera del territorio nacional.

9. Distribuidor: la persona natural o jurídica que forma parte de la cadena de suministro, distinta del proveedor o del importador, que comercializa un sistema de IA en el mercado nacional sin influir sobre sus propiedades.

10. Operador: el proveedor, el implementador, el representante autorizado, el importador y/o el distribuidor.

11. Puesta en servicio: el suministro de un sistema de IA para su primer uso directamente por parte del implementador o para uso propio en el mercado nacional, a título gratuito u oneroso, de acuerdo con su finalidad prevista.

12. Identificación biométrica: el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual para determinar la identidad de una persona, por vía de comparar sus datos biométricos con otros almacenados en una base de datos.

13. Sistema de identificación biométrica remota: aquel sistema de IA destinado a identificar a personas naturales a distancia, y comparar sus datos biométricos con los que figuran en una base de datos de referencia, sin que el operador del sistema de IA sepa de antemano si la persona en cuestión se encuentra en dicha base de datos y puede ser identificada.

14. Sistema de identificación biométrica remota en tiempo real: aquel en el que la recogida de los datos biométricos, su comparación y la identificación de una persona se producen sin una demora significativa.

15. Sistema de reconocimiento de emociones: aquel sistema de IA destinado a detectar o deducir las emociones, los pensamientos, los estados de ánimo o las intenciones de individuos o grupos a partir de sus datos biométricos y de otras técnicas,

cuyo uso vulnere los derechos fundamentales de las personas.

16. Incidente: el uso de un sistema de IA que produzca alguna de las siguientes consecuencias:

a) el fallecimiento de una persona o daños graves a su salud.

b) la alteración grave de la gestión y el funcionamiento de servicios de utilidad pública o cuya paralización cause grave daño a la salud de las personas, a la economía del país, al abastecimiento de la población o a la seguridad nacional; o bien a aquellas declaradas como infraestructura crítica, conforme con el párrafo segundo del numeral 21° del artículo 32 de la Constitución Política de la República.

c) la vulneración de derechos fundamentales protegidos por la Constitución y las leyes.

d) Daño en la persona o propiedad de otro, o daño ambiental, en los términos de la letra e) del artículo 2 de la ley N° 19.300, que aprueba ley sobre bases generales del medio ambiente.

e) la vulneración de derechos de autor y conexos.

17. Espacio controlado de pruebas: aquel entorno controlado que facilita el desarrollo, la prueba y la validación de sistemas de IA.

18. Espacio de acceso público: aquel lugar físico de propiedad pública o privada que es accesible para el público, con independencia de que deban cumplirse determinadas condiciones para su acceso y con independencia de eventuales restricciones de aforo.

19. Categorización biométrica: clasificación de personas según categorías concretas, o inferencia de sus características y atributos, en función de sus datos biométricos y sus datos de base biométrica, o que pueden inferirse a partir de dichos datos.

20. Componente de seguridad de un producto o sistema de IA: aquel que cumple una función de seguridad para dicho producto o sistema, o cuya falla o defecto de funcionamiento genera un incidente.

21. Uso indebido razonablemente previsible: la utilización de un sistema de IA de un modo que no corresponde a su finalidad prevista indicada en las instrucciones de uso establecidas por el proveedor, pero que puede derivarse de un comportamiento humano o de una interacción con otros sistemas, incluidos otros sistemas de IA, razonablemente previsible.

22. Finalidad prevista: el uso para el que un operador concibe un sistema de IA, incluido el contexto y las condiciones de uso concretas, según la información facilitada en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

Artículo 4.- Principios aplicables a los sistemas de IA. Todos los operadores a los que se aplica la presente ley deberán observar los siguientes principios generales:

1. Intervención y supervisión humana: los sistemas de IA se desarrollarán y utilizarán como una herramienta al servicio del ser humano, que respeta la dignidad humana y la autonomía personal, y que funciona de manera que pueda ser controlada y vigilada adecuadamente por seres humanos.

2. Solidez y seguridad técnica: los sistemas de IA se desarrollarán y utilizarán de manera que se minimicen los daños previsibles, y serán resistentes técnicamente frente a fallas imprevistas como frente a intentos de modificación del uso o rendimiento del sistema de IA con fines ilícitos por parte de terceros.

3. Privacidad y gobernanza de datos: los sistemas de IA se desarrollarán y utilizarán de conformidad con las normas vigentes en materia de

privacidad y protección de datos personales, y se propiciará que el tratamiento de datos cumpla con la normativa en términos de calidad e integridad. Del mismo modo, en los sistemas de IA de la administración del Estado se procurará que los datos que utilicen sean interoperables.

4. Transparencia e identificación: Los sistemas de IA se desarrollarán y utilizarán de manera que se facilite una trazabilidad adecuada, de acuerdo con lo dispuesto en el ordenamiento jurídico vigente. Además, deberán identificarse como agentes artificiales en cada oportunidad en que interactúen con seres humanos, de modo tal que éstos puedan conocer de forma clara y precisa y sean conscientes de que se comunican o interactúan con un sistema de IA.

5. Diversidad y equidad social: los usos de sistema de IA deben ser accesibles y justos para todos los grupos de la sociedad, con resguardo de los derechos fundamentales de las personas para evitar prácticas que refuercen desigualdades, discriminaciones arbitrarias o ilegales.

6. Bienestar social y medioambiental: los sistemas de IA se desarrollarán y utilizarán de manera sustentable y respetuosa con los seres humanos y el medio ambiente. Por lo anterior, los responsables de la introducción en el mercado, la puesta en servicio o la utilización de los sistemas de IA deberán revisar los efectos a largo plazo que

su aplicación genera en la sociedad, la democracia y el medio ambiente. Para esto, los operadores de sistemas de IA deberán publicar informes anuales sobre al impacto medioambiental en los canales de difusión de que dispongan, incluidas redes sociales y páginas web.

————————7. Rendición de cuentas y responsabilidad: los sistemas de IA deberán proporcionar un correcto funcionamiento a lo largo de su ciclo de vida por parte de quienes los diseñan, desarrollan, operan o despliegan, en relación con sus funciones propias y/o su utilización.

8. Protección de los derechos de los consumidores: los sistemas de IA se desarrollarán y utilizarán de conformidad con las normas vigentes en materia de protección de los derechos de los consumidores; deberán asegurar el trato justo, entrega de información veraz, oportuna y transparente y el resguardo a la libertad de elección y la seguridad en el consumo.

9. Equidad de género: se propenderá a que los sistemas de IA se desarrollen y utilicen como una herramienta para la promoción de la igualdad de género y para la eliminación de cualquier discriminación ilegal o arbitraria o violencia basada en el género. Los algoritmos, especialmente aquellos generativos, deberán diseñarse de manera tal que eviten la reproducción de las desigualdades de género existentes.

10. Protección de los derechos de autor: los sistemas de IA se desarrollarán y utilizarán de conformidad con las normas vigentes en materia de propiedad intelectual.

11. Explicabilidad: Los sistemas de IA se crearán, desarrollarán, innovarán, implementarán y usarán de manera que sus resultados o salidas sean comprensibles e inteligibles para las personas a las que impacte; y se promoverá la transparencia y la trazabilidad en todas sus operaciones.

El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, la Agencia de Protección de Datos Personales (en adelante “APDP”) y la Agencia Nacional de Ciberseguridad (en adelante “ANCI”), incorporarán estos principios en las distintas orientaciones destinadas a prestar asistencia al operador en cuanto al modo de desarrollar y utilizar sistemas de IA, así como al momento de regular y fiscalizar en sus esferas de competencia. Lo anterior se entenderá sin perjuicio de las directrices y lineamientos sobre esta materia que la Secretaría de Gobierno Digital del Ministerio de Hacienda pueda dictar en el ámbito de sus potestades legales, y de las competencias radicadas en el Consejo para la Transparencia de conformidad a lo dispuesto en la ley N° 20.285 sobre acceso a la información pública.

Artículo 5.- Obligaciones de transparencia en determinados sistemas de IA. Todo operador de

sistemas de IA que generen contenido sintético de audio, imagen, video o texto, velará porque sus resultados o salidas sean identificables como generados o manipulados de manera artificial.

Artículo 6.- Clasificación de los usos de sistemas de IA. Los usos de los sistemas de IA se clasifican, de acuerdo con su riesgo, en las siguientes categorías:

1. Usos de riesgo inaceptable: aquellos que resultan incompatibles con el respeto y garantía de los derechos fundamentales de las personas, establecidos en el artículo 7. Se prohíbe la distribución, introducción en el mercado o puesta en servicio de sistemas de IA destinados a tales usos.

2. Usos de alto riesgo: aquellos usos de sistemas de IA autónomos o componentes de seguridad de productos cuya utilización presenta un riesgo significativo de afectación a los derechos fundamentales de las personas, especialmente si estos sistemas fallan o se utilizan de forma impropia.

3. Uso de riesgo limitado: aquellos que presentan riesgos no significativos de manipulación, engaño o error, producto de su interacción con personas.

4. Usos sin riesgo evidente: todos los demás usos que no entran en las categorías

precedentes.

Para los efectos de esta ley, se entenderá por “uso” el desarrollo, prueba y validación de los sistemas de IA, así como su distribución, introducción en el mercado, puesta en servicio, o cualquier actividad realizada por un operador.

TÍTULO II
USOS DE RIESGO INACEPTABLE DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Artículo 7.- Usos de riesgo inaceptable de sistemas de IA. Serán aquellos comprendidos en algunas de las siguientes categorías:

1. Manipulación subliminal: sistemas de IA que emplean técnicas imperceptibles para las personas y que tienen como objeto la inducción de acciones que causan daños a la salud física o mental. En particular, se prohíben los usos de sistemas de IA que, mediante manipulación o engaño, tengan por finalidad o efecto alterar el comportamiento de una o más personas, menoscabar su capacidad de decisión informada e inducir la adopción de decisiones que razonablemente no habrían tomado en ausencia de ellas.

Esta prohibición no se aplicará a los sistemas de IA destinados a fines terapéuticos siempre que sea realizado conforme a la ley. En estos casos se requerirá el consentimiento informado específico y expreso de la persona.

2. Explotación de características de las personas para generar comportamientos dañinos: sistemas de IA que aprovechan o explotan características conocidas de las personas, como los rasgos de la personalidad, situación social o económica, rango etario, información relativa a la vida sexual, orientación sexual, identidad de género, la capacidad física o mental, entre otras, que tengan por objeto alterar de manera sustancial su comportamiento o limitar su voluntad, con vulneración de sus derechos fundamentales o provocación de perjuicios a las personas.

Asimismo, se entenderán incluidos dentro de esta categoría aquellos usos de sistemas de IA que sean dañinos o afecten la honra, la integridad y el libre desarrollo de la sexualidad de las personas, en particular, aquellos cuyos usos puedan significar una vulneración de los derechos de niños, niñas y adolescentes, de acuerdo con lo dispuesto en la ley N° 21.430, sobre garantías y protección integral de los derechos de la niñez y adolescencia.

3. Categorización de personas basada en datos personales sensibles: sistemas de categorización biométrica u otras técnicas de tratamiento de datos que clasifiquen e identifiquen a personas naturales con arreglo a datos personales sensibles, o que partan de la base de una inferencia respecto de dichos atributos o características, de modo tal que dicha categorización provoque una discriminación ilegal o arbitraria.

Esta prohibición no se aplicará a los sistemas de IA destinados a ser utilizados para fines terapéuticos autorizados sobre la base de un consentimiento informado, específico y expreso por parte de las personas naturales expuestas a ellos o, en su caso, de su representante legal o judicial. Además, se requerirá la autorización sanitaria respectiva, de ser procedente.

4. Calificación social genérica: sistemas de IA que tienen por finalidad evaluar o clasificar a personas o grupos de personas naturales en función de su comportamiento social, su nivel socioeconómico o sus características personales o de personalidad conocidas o inferidas, de modo tal que su calificación resultante provoque una discriminación ilegal o arbitraria respecto de dichas personas o grupos de personas.

5. Identificación biométrica remota en tiempo real en espacios de acceso público: sistemas de IA utilizados para el análisis de imágenes de video en espacios de acceso público que emplean sistemas de identificación biométrica remota en tiempo real.

6. Extracción no selectiva de imágenes faciales: sistemas de IA que crean o amplían bases de datos de reconocimiento facial mediante la extracción indiscriminada, masiva y sin el consentimiento de las personas, de imágenes faciales a partir de internet o desde un circuito cerrado de televisión.

7. Evaluación de los estados emocionales de una persona: sistemas de IA que pretenden inferir las emociones de una persona natural en los ámbitos de la aplicación de la ley penal, procesal penal y de la gestión de fronteras, en lugares de trabajo y en centros educativos.

TÍTULO III
USO DE ALTO RIESGO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Artículo 8.- Uso de alto riesgo de Sistemas de IA. La utilización de un sistema de IA se considerará de alto riesgo cuando presente un riesgo significativo de afectación de los derechos fundamentales protegidos por la Constitución Política de la República, así como de los derechos del consumidor, de autor y conexos, ya sea que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto, o bien que sea en sí mismo dicho producto.

El uso de alto riesgo de sistemas de IA deberá procurar el respeto de los derechos fundamentales de las personas. Del mismo modo, deberán prevenir la creación de estereotipos, así como la degradación de personas o grupos de personas que interactúan con este tipo de sistemas de IA.

— Artículo 9.- Reglas aplicables. Los

sistemas de IA cuyos usos sean calificados de alto riesgo deberán cumplir con las siguientes reglas:

1. Establecimiento de sistemas de gestión de riesgos: Se someterán a un proceso iterativo continuo de evaluación de riesgos que se llevará a cabo durante todo el ciclo de vida del sistema, el cual requerirá revisiones y actualizaciones periódicas para procurar su eficacia y minimizar las posibilidades de falla o mal funcionamiento, según la finalidad prevista declarada.

El sistema de gestión de riesgos podrá integrarse en procedimientos de gestión de riesgos ya existentes, o en parte de ellos que el operador haya implementado por exigirlo así la ley o la autoridad respectiva, e incorporará las medidas frente a incidentes aplicables al sistema de IA en caso de fallas o mal funcionamiento.

2. Gobernanza de datos: Si utilizan técnicas de entrenamiento de modelos con datos deberán contar con una gobernanza de datos adecuada a su propósito y contexto de uso.

Asimismo, deberán incorporar estándares de seguridad y protección de datos, e incluir mecanismos de prevención y gestión de incidentes de seguridad de la información, según su ámbito de aplicación.

3. Documentación técnica: La documentación técnica requerida será inteligible y se redactará de modo tal que demuestre que cumple con

las reglas establecidas en esta ley.

4. Sistema de registros: Deberán contar con funciones que permitan registrar información y eventos de seguridad mientras están en funcionamiento.

Los registros deberán almacenarse con medidas de seguridad adecuadas para evitar su alteración, pérdida o acceso no autorizado. Su acceso estará restringido a personal autorizado y a la autoridad fiscalizadora competente.

5. Mecanismos de supervisión humana: Deberán contar con mecanismos técnicos y operativos que permitan su supervisión por personas naturales técnicamente capacitadas para esta función, de forma idónea y proporcional. La supervisión deberá garantizar que el sistema se utilice conforme a su finalidad prevista y, además, identificar y mitigar los riesgos asociados a un uso indebido razonablemente previsible, con el fin de evitar impactos negativos en los derechos fundamentales de las personas.

6. Precisión, solidez y ciberseguridad: El funcionamiento de estos sistemas deberá respetar el principio de seguridad desde el diseño y por defecto, contar con un nivel adecuado de precisión, resiliencia, seguridad y ciberseguridad, funcionar de manera fiable, predecible y resiliente, y garantizar su seguridad y resistencia a incidentes durante todo su ciclo de vida.

El cumplimiento de estos requisitos deberá garantizarse mediante la implementación de medidas de seguridad alineadas con lo dispuesto en los artículos 3, 7 y 9 de la ley N° 21.663, ley marco de ciberseguridad.

En cualquier caso, para el cumplimiento de las reglas precedentes se podrán establecer estándares diferenciados en virtud del tipo y tamaño del operador. Se tendrá especial consideración en las características y necesidades de las empresas de menor tamaño, tal como se definen en la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.

Cuando el uso de alto riesgo de un sistema de IA no se ajuste a las reglas previstas en esta ley, el operador adoptará inmediatamente las medidas necesarias para desactivarlo, retirarlo del mercado o suspenderlo. Estas medidas se encontrarán establecidas dentro del sistema de gestión de riesgos referido y serán diseñadas de conformidad con su finalidad de uso.

La APDP y la ANCI, en el ámbito de sus competencias, podrán requerir a los operadores de estos sistemas procedimientos específicos de fiscalización, respecto a la materia regulada en esta ley, cuando existan indicios de incumplimiento de la normativa vigente o riesgos potenciales para el ejercicio de los derechos fundamentales.

Artículo 10.- Seguimiento posterior a la implementación, puesta en servicio, distribución e introducción en el mercado de usos de sistemas de IA de alto riesgo. Los operadores establecerán y documentarán un sistema de seguimiento, que sea proporcional y adecuado a la naturaleza y riesgos identificados en sus usos.

El sistema de seguimiento recabará y analizará datos proporcionados por los operadores o recopilados a través de otras fuentes, con el objetivo de evaluar el funcionamiento de los usos de sistemas de IA de alto riesgo durante toda su vida útil. Este proceso permitirá a los operadores determinar el nivel de cumplimiento de las reglas del artículo 9.

Cuando proceda, el seguimiento posterior incluirá un análisis de la interacción con otros entornos de sistemas de IA, incluidos otros dispositivos y *software* interconectados que puedan influir en su funcionamiento o generar riesgos adicionales.

TÍTULO IV
USOS DE RIESGO LIMITADO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Artículo 11.- Uso de riesgo limitado de Sistemas de IA. La utilización de un sistema se considerará de riesgo limitado si presenta un riesgo no significativo de manipulación, engaño o error,

producto de su interacción con personas.

— Los sistemas de IA de riesgo limitado deberán garantizar condiciones de transparencia y seguridad proporcionales a su nivel de riesgo, de modo tal que las personas sean informadas de forma clara y precisa y les permitan reconocer que están interactuando con un sistema de IA.

TÍTULO V
MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 12.- Responsabilidad generada a partir de espacios controlados de pruebas para la IA. Los operadores en los espacios controlados de pruebas para la IA responderán de cualquier perjuicio causado a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas.

— Siempre que los operadores respeten las disposiciones de esta ley y las orientaciones proporcionadas por los órganos de la Administración del Estado que habiliten estos espacios controlados de prueba, estarán exentos del pago de las multas administrativas a las que se refiere el artículo 17, sin perjuicio de la responsabilidad por los daños que puedan causar.

La utilización de un espacio controlado de prueba no es un requisito habilitante para el desarrollo, prueba y validación de los sistemas de IA, ni para su distribución, introducción en el

mercado, puesta en servicio, ni para cualquier actividad realizada por un operador, y no exime de las obligaciones y responsabilidades establecidas en esta ley.

Articulo 13.- Medidas dirigidas a empresas de menor tamaño y a organizaciones de la sociedad civil. El Estado, a través de los ministerios de Ciencia, Tecnología, Conocimiento e Innovación y de Economía, Fomento y Turismo, propiciará medidas tendientes a:

1. Proporcionar a las empresas de menor tamaño establecidas en el territorio nacional un acceso prioritario a los espacios controlados de pruebas para la IA existentes, todo ello con arreglo a la disponibilidad presupuestaria existente.

2. Promover la realización de iniciativas de sensibilización, creación de capacidades y desarrollo de competencias digitales avanzadas en materia de usos vinculados a la IA, adaptadas a las necesidades de las empresas de menor tamaño.

Las medidas señaladas en el inciso anterior se dirigirán a organizaciones de la sociedad civil que desarrollen o utilicen sistemas de IA, con arreglo a criterios objetivos, públicos y no discriminatorios.

Artículo 14.- El Ministerio de Ciencia,

Tecnología, Conocimiento e Innovación, en el marco de sus funciones y atribuciones, en coordinación con el Ministerio de Economía, Fomento y Turismo, promoverá el desarrollo ético y responsable de la inteligencia artificial en el país, con pleno respeto a los derechos fundamentales garantizados por la Constitución y las leyes, y establecerá medidas de apoyo a la innovación basada en sistemas de IA. Para ello, podrá solicitar la colaboración de entidades o personas del sector privado, y de universidades del país, conforme a lo dispuesto en las letras f) y m) del artículo 5º de la ley Nº 21.105.

Le corresponderá especialmente al Ministerio de Ciencia, Tecnología, Conocimiento e Innovación promover, diseñar y elaborar programas orientados a la alfabetización y divulgación ciudadana en materia de IA, y velar por la creación de instrumentos que permitan la comprensión de la tecnología y eduquen acerca de los derechos y obligaciones respecto a los usos de los sistemas de IA en los términos contenidos en esta ley, sus ventajas, potencialidades y riesgos.

TÍTULO VI
CONFIDENCIALIDAD, INFRACCIONES Y SANCIONES

Artículo 15.- Confidencialidad en el uso de sistemas de IA. Las personas naturales, las personas jurídicas y los órganos de la administración del Estado involucrados en la aplicación de la presente ley deberán respetar la confidencialidad de la información y los datos obtenidos de un sistema de IA

en el ejercicio de sus funciones y actividades, de modo que se protejan, en particular:

1.— Los derechos de propiedad intelectual e industrial y la información empresarial confidencial y los secretos comerciales de una persona natural o jurídica, incluido el código fuente.

2. Los datos personales y su tratamiento de conformidad con la normativa vigente.

3. El interés público y la seguridad nacional.

————————4. La integridad de las causas penales o los procedimientos administrativos.

Lo anterior, sin perjuicio de otras leyes que resulten aplicables que regulen el acceso, tratamiento y protección de esta información.

Artículo 16.- Infracciones. Para efectos del ejercicio de las atribuciones de la Agencia de Protección de Datos Personales, se considerará como infracción:

1. Gravísima: El uso de un sistema de IA por parte de un operador, que contravenga lo dispuesto en el artículo 7 sobre usos de riesgo inaceptable. Se considerará además infracción gravísima la reincidencia de una misma infracción

grave dentro de un año.

2. Grave: el incumplimiento, por parte de un operador, de las reglas dispuestas en el artículo 9 para los usos de alto riesgo. Se considerará además infracción grave la reincidencia en una misma infracción leve dentro de un año.

3. Leve: el incumplimiento, por parte de un operador, de las obligaciones de transparencia dispuestas respecto de los usos de riesgo limitado regulados en el artículo 11. Se considerará además infracción leve cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción específica.

Las sanciones dispuestas en este artículo se aplicarán sin perjuicio de las disposiciones de la ley N° 21.719, en caso de que la infracción involucre el tratamiento de datos personales y resulte aplicable su régimen sancionatorio.

Artículo 17.- Sanciones. La infracción a los preceptos de esta ley será sancionada de la siguiente manera:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales.

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades

tributarias mensuales.

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales.

En la determinación de la cuantía de la multa administrativa se tomarán en consideración, en cada caso concreto, todas las circunstancias pertinentes de la situación particular, y se tendrá debidamente en cuenta:

a) La duración de la infracción y sus consecuencias, atendido el propósito del uso y alcance del sistema de IA, y, cuando proceda, la gravedad, intensidad, probabilidad de ocurrencia y duración de sus efectos, así como el número de personas afectadas y el nivel de los daños ocasionados.

b) El tamaño y volumen de las ventas anuales del operador que comete la infracción.

c) Las acciones emprendidas por el operador para mitigar los perjuicios o los daños sufridos por las personas.

d) El grado de cooperación del operador con las autoridades nacionales competentes con el fin de remediar la infracción y mitigar sus posibles efectos adversos.

e) El rol específico que cumple el

proveedor, implementador, representante autorizado, importador y/o distribuidor en la cadena de valor de la inteligencia artificial.

f) El beneficio económico obtenido con la infracción.

g) La reincidencia del infractor.

Cuando por unos mismos hechos y fundamentos jurídicos, el infractor pueda ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.

Artículo 18.- Responsabilidad civil. La persona que sufra un daño como consecuencia de la utilización de un sistema de IA, podrá demandar civilmente:

1. La cesación de los actos generadores de daño.

2. La indemnización de los daños y perjuicios.

3. La adopción de las medidas necesarias para evitar que prosiga la infracción, cuando exista peligro inminente de daño irreparable.

4. La publicación de la sentencia a costa del condenado, mediante anuncios en un diario a

elección del demandante. Esta medida será aplicable cuando la sentencia así lo señale expresamente.

Las responsabilidades en que incurra una persona natural o jurídica por las infracciones establecidas en esta ley se entienden sin perjuicio de las demás responsabilidades legales, civiles y penales que puedan corresponderle de acuerdo a la normativa vigente.

Artículo 19.- Procedimiento aplicable en materia civil. La acción civil establecida en el artículo 18 se tramitará conforme al procedimiento sumario, de conformidad a las disposiciones del Título XI del Libro Tercero del Código de Procedimiento Civil.

Artículo transitorio.- Las normas de la presente ley entrarán en vigencia el primer día hábil del duodécimo mes desde su publicación en el Diario Oficial.

*****

Lo que tengo a honra comunicar a V.E.

JOSÉ MIGUEL CASTRO BASCUÑÁN
Presidente de la Cámara de Diputados

MIGUEL LANDEROS PERKIĆ
Secretario General de la Cámara de Diputados