REPUBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

MENSAJE DE S.E. EL PRESIDENTE DE LA REPÚBLICA POR EL QUE INICIA UN PROYECTO DE LEY DE INTELIGENCIA ARTIFICIAL.

Santiago, 7 de mayo de 2024

M E N S A J E N° 063-372/

A S.E. LA PRESIDENTA DE LA H. CÁMARA DE DIPUTADAS Y DIPUTADOS

Honorable Cámara de Diputadas y Diputados:

En uso de mis facultades constitucionales, someto a vuestra consideración el presente proyecto de ley de inteligencia artificial.

I. **ANTECEDENTES**

La inteligencia artificial (IA) es un conjunto de sistemas basado en máquinas que infieren, a partir de información de entrada, determinada información de salida, que puede consistir en predicciones, contenidos, recomendaciones o decisiones capaces de influenciar espacios físicos o virtuales.

La rápida y reciente evolución de los usos de sistemas de IA ha generado un impacto transversal sobre toda la sociedad, tanto a nivel nacional como en el contexto global. Aunque es un campo que existe desde hace años, aplicaciones que antes eran difícilmente imaginables en su desempeño han ido apareciendo a un ritmo sin precedentes.

En este contexto, la IA ofrece un extraordinario potencial para incrementar el bienestar de las personas, por la vía de acceder a nuevos descubrimientos

científicos que amplían los límites del conocimiento humano; optimizar el uso de recursos finitos que nos ayudan en tareas cotidianas; y ampliar el acceso a la educación, así como al goce de diversos derechos fundamentales, sólo por mencionar algunos beneficios. En último término, la IA puede contribuir de manera significativa en la transición de los países hacia un futuro socialmente más justo y ecológico de la mano de la tecnología.

En el ámbito económico, la IA puede facilitar la consecución de resultados positivos desde el punto de vista social y medioambiental, mediante la mejora de la predicción, la optimización de las operaciones, la asignación de los recursos y la personalización de la prestación de servicios, proporcionando grandes ventajas competitivas a las empresas y la economía nacional. Esto es especialmente necesario en sectores de gran impacto como el cambio climático, el medio ambiente y la salud, el sector público, las finanzas, la movilidad y la agricultura.

Para que dichos beneficios se materialicen, es crucial garantizar que la IA se desarrolle y utilice de forma ética y responsable. Estos sistemas se encuentran al servicio de las personas y, en tal calidad, deben observar valores y principios rectores que orienten tanto sus usos, como el diseño de políticas públicas a su respecto. Entre ellos, es fundamental el respeto, protección y promoción de los derechos fundamentales y de principios matrices como la supervisión humana, la transparencia y explicabilidad, la diversidad, no discriminación y equidad, la protección de datos personales, el bienestar social y medioambiental, así como la responsabilidad, sólo por mencionar algunos.

Por otra parte, los mismos elementos y técnicas que potencian los beneficios

socioeconómicos de la IA también pueden dar lugar a nuevos riesgos o consecuencias negativas para las personas o la sociedad en su conjunto. Por ejemplo, usos inadecuados de este tipo de sistemas pueden reforzar prejuicios y sesgos respecto a personas o determinados grupos de personas. En este sentido, la velocidad, autonomía y opacidad de los sistemas de IA desafían los modelos tradicionales de regulación.

En este contexto, la provisión de certezas regulatorias sobre los sistemas de IA que permitan su investigación, desarrollo e implementación, respetando los derechos fundamentales de las personas, se vuelve indispensable.

1. Recomendación de la UNESCO sobre la ética de la IA

Durante noviembre del año 2021, UNESCO emitió la Recomendación sobre la ética de la IA como una reflexión para guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos y desconocidos de las tecnologías de la IA. Para evaluar la factibilidad de su implementación, UNESCO desarrolló una metodología (“RAM” por sus siglas en inglés) creada para ayudar a los Estados a identificar su nivel de preparación y, al mismo tiempo, proporcionar una base para que la UNESCO adapte su apoyo al desarrollo de capacidades.

Chile es el primer país en el mundo en implementar la RAM, en la que participaron más de 300 personas en 7 mesas de discusión. Los resultados obtenidos dieron paso a la Actualización de la Política Nacional de Inteligencia Artificial por parte del Ministerio de Ciencia Tecnología Conocimiento e Innovación (MCTCI), iniciada en el año 2023, así como a la necesidad de avanzar en diversas iniciativas regulatorias.

2. Actualización de la Política Nacional de IA

Durante el año 2019, un grupo de carteras de Estado lideradas por el MCTCI presentó un diagnóstico sobre la necesidad de elaborar una Política Nacional de IA, el que fue complementado por la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación de este Honorable Senado, que estuvo de acuerdo en la necesidad de generar una hoja de ruta para potenciar la investigación y desarrollo (I+D) en IA, la innovación y la captura de sus beneficios sociales y económicos.

Dicho proceso culminó en la publicación de la Política Nacional de IA del año 2021, la que entrega una serie de lineamientos estratégicos en los que se debe enfocar el país en materia de IA durante los próximos 10 años.

Desde entonces, el país ha sido testigo de significativos avances en la materia: la creación del Centro Nacional de Inteligencia Artificial (CENIA); la focalización en IA de becas de postgrado entregadas por la Agencia Nacional de Investigación y Desarrollo (ANID); la puesta en marcha de las redes de 5G; y el primer doctorado de IA en Chile y Latinoamérica, entre otros hitos. Ello ha posicionado a Chile como un referente en la región en materia de IA, particularmente en infraestructura para datos, capital humano avanzado e investigación y conectividad (CENIA, 2023).

Ahora bien, aun cuando la Política Nacional de IA sigue vigente, el acelerado avance de las tecnologías basadas en sistemas de IA motivó, desde el Ministerio de CTCI, una actualización de su eje de Gobernanza y Ética, incorporando diversos espacios participativos y recomendaciones de diversos organismos públicos y

privados, instituciones de educación superior y miembros de la sociedad civil.

En línea con lo recién señalado, el Ministerio de CTCI también actualizó el plan de acción que se deriva de la Política Nacional de IA, poniendo especial énfasis en acciones que apunten al desarrollo y adopción de sistemas de IA, poniendo en el centro a las personas y el resguardo de sus derechos fundamentales.

3. Circular sobre uso responsable de herramientas de IA en el sector público

Otro antecedente relevante fue la dictación por parte del Ministerio Secretaría General de la Presidencia y el Ministerio de CTCI, de la circular sobre uso responsable de herramientas de IA en el sector público, en el mes de diciembre de 2023 (la “circular”).

Dicho instrumento de política pública, además de servir de orientación a los órganos de la administración del Estado en materia de adopción y uso responsable de sistemas de IA, permitirá medir de manera preliminar el nivel de penetración de este tipo de tecnologías en el sector público y su utilidad para satisfacer necesidades públicas en beneficio de la ciudadanía.

4. Trabajo de la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado

Adicionalmente, otro antecedente relevante de esta iniciativa ha sido el trabajo desempeñado por la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación de este H. Senado durante el 2023 en materia de IA, a partir de la conformación de la mesa técnica de trabajo en materia de Inteligencia Artificial.

Cabe destacar que esta iniciativa generada desde el H. Senado convocó a más de 120 profesionales de diversas disciplinas, desde filósofos, periodistas, sociólogos, hasta ingenieros, expertos en base de datos e inteligencia artificial.

5. Trabajo de la Comisión de Futuro, Ciencia, Tecnología, Conocimiento e Innovación de la H. Cámara de Diputadas y Diputados

Sumado a lo anterior, hay que añadir el trabajo desempeñado por la Comisión de Futuro, Ciencia, Tecnología, Conocimiento e Innovación de la H. Cámara de Diputadas y Diputados a lo largo de todo el año 2023, a partir del proyecto de ley boletín N°15869-19, que regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación.

6. Experiencia comparada

En el escenario internacional se han promovido distintos niveles de acercamiento a la regulación de IA. A continuación, se presenta un resumen de los más relevantes:

- **Unión Europea**: La Ley de Inteligencia Artificial de la Unión Europea, adoptada en marzo recién pasado, asigna regulaciones proporcionales al nivel de riesgo que presenta una herramienta de IA. Su objetivo apunta a crear una escala proporcional de regulaciones diseñada para asignar restricciones más estrictas a los sistemas de IA más riesgosos. Esta legislación pretende categorizar las herramientas de inteligencia artificial con base en cuatro designaciones: riesgo inaceptable, alto, limitado y mínimo.

- **Estados Unidos de Norteamérica**: El gobierno del presidente Joe Biden les ha dado a las empresas tecnológicas cierto espacio para adoptar compromisos

voluntarios de control, enfocados en riesgos de seguridad. En julio de 2023, se anunció que varias creadoras de IA, como Amazon, Anthropic, Google, Inflection, Meta, Microsoft y OpenAI, convinieron aplicar sus propias regulaciones a sus sistemas de IA, en línea con la estrategia del gobierno de los Estados Unidos de Norteamérica de promover la autorregulación sobre los usos asociados a esta tecnología.

Los compromisos incluyen la realización de pruebas por terceros a las herramientas, conocido como simulacro de ciberataque; investigación en temas de sesgo y privacidad; intercambio de información sobre riesgos con gobiernos y otras organizaciones y desarrollo de herramientas para combatir retos de la sociedad como el cambio climático, además de incluir medidas para garantizar la transparencia y así poder identificar el material generado por IA. Estas empresas ya tendrían en marcha muchas de esas acciones.

- **China**: Desde 2021, China ha actuado con agilidad para poner en vigor regulaciones sobre algoritmos de recomendación, contenido sintético como las imágenes ultrafalsas e inteligencia artificial generativa. Estas normas prohíben la discriminación de precios por los algoritmos de recomendación en las redes sociales, por ejemplo. Los productores de IA deben identificar el contenido sintético generado por IA. Por último, en cuanto a las normas preliminares para la inteligencia artificial generativa, se requiere que los datos de entrenamiento y el contenido creado por la tecnología sean “ciertos y precisos”.

- **Ámbitos de cooperación global**: Algunos expertos convocados por organismos multilaterales han comentado que, para elaborar una regulación efectiva aplicable

a la inteligencia artificial, podría ser necesaria una convergencia y colaboración mundial. Así por ejemplo, encontramos al Grupo de Trabajo Interinstitucional sobre Inteligencia Artificial, codirigido por la Unión Internacional de Telecomunicaciones (UIT) y UNESCO e integrado por diversas entidades del sistema de las Naciones Unidas, quien en abril de 2024 publicó un *white paper* sobre gobernanza de la IA bajo el sistema de Naciones Unidas como una forma de análisis de los modelos institucionales actuales así como de los marcos normativos internacionales existentes en el sistema de Naciones Unidas que podrían aplicarse o aprovecharse de cara a un ámbito de gobernanza internacional de la IA.

I. **FUNDAMENTOS**

1. Aspectos generales

La revolución tecnológica en curso obliga a acelerar nuestra adaptación a los cambios producidos por la masificación de tecnologías y sus usos. Dado que la IA es una tecnología de propósito general y su impacto es transversal a las oportunidades del futuro a nivel cultural, social y económico, es clave empoderarnos en su desarrollo y empleo.

Sin embargo, dado el avance vertiginoso de esta tecnología, más allá de los enormes beneficios que puede reportar a nivel social, económico y cultural, han surgido diversos riesgos a abordar, especialmente para mitigar posibles efectos que menoscaben el ordenamiento jurídico. Por este motivo, el proyecto plantea un marco jurídico para regular los distintos usos de los sistemas de inteligencia artificial, para impulsar el desarrollo, la utilización y la adopción de esta tecnología con el propósito de promover procesos de innovación y, al mismo tiempo, resguardar

los derechos fundamentales de las personas.

2. El alcance general de los sistemas de IA

El alcance transversal de los sistemas de IA obliga a pensar marcos normativos que confieran seguridad jurídica a quienes participan de su diseño, desarrollo, comercialización y puesta en servicio y, al mismo tiempo, la flexibilidad necesaria para adaptarse a los avances tecnológicos en esta materia.

Al respecto, la OCDE en 2023 ha provisto una definición actualizada de sistemas de IA que se basa en sus características funcionales y, particularmente, en su capacidad para generar, sobre un conjunto concreto de objetivos definidos por seres humanos, contenidos, predicciones, recomendaciones, decisiones u otra información de salida que influye en el entorno con el que interactúa el sistema, ya sea en una dimensión física o digital. Esto implica que los sistemas de IA pueden diseñarse para operar con distintos niveles de autonomía y utilizarse de manera independiente o como componentes de un producto, con independencia de si el sistema forma parte físicamente de él (sistema integrado) o tiene una funcionalidad en el producto sin formar parte de él (sistema no integrado).

Por lo mismo, dada la plasticidad y la amplitud de esta tecnología y sus usos, este proyecto tiene como punto de partida la definición señalada, para delimitar apropiadamente su ámbito de aplicación y al mismo tiempo, permitir su adaptación a la evolución en la utilización de los sistemas de IA.

3. Protección frente a la afectación de derechos fundamentales y regulación en base a riesgos

Para promover la adopción de sistemas de inteligencia artificial centrados en el ser humano es fundamental garantizar la protección de la salud, la seguridad y los derechos fundamentales de las personas, así como la protección de los consumidores frente a los efectos nocivos que determinados usos pudieran irrogar. Por ello que su desarrollo y utilización debe circunscribirse a un marco ético común.

Bajo esta premisa, en la esfera pública comparada y nacional se han identificado usos vinculados a sistemas de IA cuyos riesgos de infracción a los valores éticos y jurídicos mencionados son de tal magnitud que se ha estimado que obstan al ordenamiento jurídico. En primer lugar, aparecen las prácticas que tienen el potencial de manipular a las personas a través de técnicas subliminales que trasciendan su consciencia. Asimismo, técnicas que aprovechan las vulnerabilidades de grupos concretos para alterar de manera sustancial su comportamiento o limitar su voluntad, de un modo que es probable que les provoque, a ellos o a terceros, perjuicios físicos o psicológicos.

De especial relevancia en el debate contemporáneo, se ha advertido sobre la posibilidad de que los sistemas de IA sean dañinos o afecten la honra, la integridad y el libre desarrollo de la sexualidad de las personas, en particular la de niños, niñas y adolescentes. Ello se debe a la particular situación de vulnerabilidad a la que pueden verse expuestos en contextos digitales, razón por la cual el Estado está llamado a resguardar y posibilitar el pleno ejercicio de sus derechos.

Otro subconjunto de situaciones de riesgo se ha identificado en los sistemas

de IA de categorización biométrica de personas basadas en datos personales sensibles, o que partan de la base de una inferencia respecto a dichos atributos o características. Estos casos refuerzan la necesidad de proteger la privacidad de las personas, prevenir el abuso de este tipo de sistemas -por ejemplo, la suplantación de identidad o la comisión de otros tipos de fraudes-, evitar la discriminación y la producción de sesgos y garantizar que se obtenga el consentimiento adecuado de los titulares de datos personales.

Algo similar sucede con algunos sistemas de identificación biométrica, de presentarse el tratamiento no autorizado de datos personales, o que se presten para la vigilancia masiva, con el consiguiente potencial de socavar el ejercicio de derechos fundamentales.

También existen riesgos para el ejercicio del derecho a la igualdad ante la ley, en particular por los riesgos de discriminación que podrían ocasionar determinados sistemas de IA en el acceso a bienes y servicios. En esta categoría figuran los sistemas de IA de calificación social genérica. Si estos son generados en función de comportamientos sociales, niveles socioeconómicos o características personales o de personalidad conocidas o inferidas de personas o grupos de personas naturales, que se traduzcan en un trato injusto o discriminatorio, su uso podría configurar una afectación de los derechos fundamentales.

Otro tanto ocurre con los sistemas de IA basados en técnicas de *facial scraping*, es decir, aquellos que crean o amplían bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales desde internet o de imágenes de circuitos cerrados de televisión, debido al riesgo de extracción

y tratamiento de datos personales sin consentimiento de sus titulares, además de su falta de transparencia y control.

Por último, un subconjunto de especial preocupación son los sistemas de IA destinados a la evaluación de los estados emocionales de una persona en los ámbitos de la aplicación de la ley penal, procesal penal y la gestión de fronteras, en lugares de trabajo y en centros educativos. El riesgo de error de dichos sistemas y, particularmente, el riesgo de vulneración de derechos respecto de los sujetos pasivos de este tipo de usos podría traducirse en mecanismos de coacción física o psíquica.

Con todo, este listado no agota todos los efectos nocivos que podrían suscitarse, puesto que también podrían presentarse otros usos de sistemas de IA que pueden llegar a causar efectos similares si fallan o se utilizan de forma impropia. Además, aunque no fallen, un sistema de IA podría arribar a resultados incorrectos o sesgados y presentar, por ello, riesgos de manipulación o engaño.

Así, de forma similar a la Ley de IA europea y a partir del consenso existente a nivel comparado en torno a la conveniencia de adoptar un enfoque basado en riesgos para la regulación de las tecnologías basadas en sistemas de IA, este proyecto de ley adopta dicho enfoque vinculado al desarrollo, implementación y uso de sistemas de IA. Reconociendo que no todos los efectos tienen una entidad equivalente en términos de su afectación de derechos fundamentales, la normativa que se propone distingue entre usos de sistemas de IA (i) de riesgo inaceptable -y que quedarán, por lo tanto, prohibidos- (ii) de alto riesgo, (iii) de riesgo limitado, y (iv) sin riesgo evidente. Para estos tres últimos grupos se disponen distintas medidas o reglas que deberán ser

adoptadas por los operadores, con mayor o menor intensidad según fuere el caso.

4. Respaldo e incentivo a la innovación

Dado que la IA agrupa a una familia de tecnologías de rápida evolución que requiere nuevas formas de vigilancia regulatoria y un espacio seguro para la experimentación, así como que se garantice la innovación responsable y la integración de salvaguardias y medidas de reducción del riesgo adecuadas. Bajo este escenario, para que Chile continúe su liderazgo en el desarrollo e implementación de sistemas de IA en América Latina, es necesario brindar a desarrolladores y operadores marcos e incentivos adecuados para la creación, desarrollo, innovación e implementación de los sistemas de IA.

En este sentido, la presente iniciativa contribuirá a la innovación por la vía principalmente de dos ejes: posibilitar los espacios controlados de pruebas para sistemas de IA y promover explícitamente las medidas dirigidas a empresas de menor tamaño en esta materia.

Respecto al primero, los organismos de la administración del Estado estarán facultados para proporcionar espacios controlados que fomenten la innovación y faciliten el desarrollo, la prueba y la validación de sistemas innovadores de IA en su esfera de competencia, durante un período limitado de tiempo antes de su introducción en el mercado o su puesta en servicio. Este espacio controlado de pruebas deberá desarrollarse con arreglo a un plan específico acordado entre los proveedores potenciales y las autoridades creadoras de tales espacios, bajo la orientación y supervisión de estas últimas. En la medida que se ajusten al plan, podrán eximirse de posibles sanciones administrativas.

Esta institución apunta a analizar la operatividad de las reglas y estándares establecidos en este proyecto, así como la evaluación de cumplimiento y la prueba de los sistemas de IA de los participantes durante su funcionamiento, de forma previa a su comercialización o puesta en servicio. De este modo, se busca reforzar la cooperación entre actores públicos y privados de cara a la generación de directrices de buenas prácticas y guías que permitan garantizar la aplicación de la regulación sobre usos de sistemas de IA en el país.

En suma, los espacios controlados de pruebas deben tener los objetivos de impulsar la innovación en el ámbito de la IA estableciendo un entorno de experimentación y prueba controlado en la fase de desarrollo y previa a la comercialización, con vistas a garantizar que los sistemas de IA innovadores cumplan lo dispuesto en la presente propuesta como también con aquellas disposiciones legales que puedan resultar aplicables; de dotar de mayor seguridad jurídica a las empresas y, al mismo tiempo, favorecer la supervisión de las autoridades competentes y su entendimiento de las oportunidades, riesgos y consecuencias del uso de las tecnologías basadas en sistemas de IA; y de acelerar el acceso a mercados por la vía de eliminar barreras burocráticas existentes.

En todo caso, con el propósito de observar un estándar de diligencia suficiente en la utilización del espacio controlado de pruebas para la IA, se establecerá que los proveedores potenciales responderán de cualquier perjuicio causado a terceros como resultado de la experimentación realizada dentro del mismo.

Respecto al segundo eje, se estimó conveniente promover medidas de apoyo a empresas de menor tamaño, como una forma de promover y proteger la innovación, teniendo

en particular consideración los intereses de los proveedores y los usuarios de sistemas de IA a pequeña escala. Dentro de ellas se encuentran el otorgar accesos prioritarios a espacios controlados de prueba para la IA existentes, la promoción del desarrollo de capacidades en materia de usos vinculados a la IA, y el fomento de la participación de representantes de empresas de menor tamaño en el Consejo Asesor Técnico de IA propuesto en esta normativa.

5. Principios, reglas y gobernanza para sistemas de IA al servicio de la persona humana

Al tratarse de una tecnología en evolución -con transformaciones rápidas y en ocasiones, impredecibles- se ha preferido un modelo que favorece estándares amplios y sencillos. Como se detalla en la sección siguiente, el título sobre principios del proyecto recoge los consensos internacionales en la materia, y en lugar de pormenorizar todas las reglas a nivel legal, da espacio a que exista normativa infralegal y otros espacios de gestión de riesgos, contando con el protagonismo de la industria y de los usuarios.

Con todo, estos principios también dan pie a reglas reforzadas, como ocurre con los sistemas de IA de alto riesgo, que deben cumplir con reglas específicas sobre mecanismos de supervisión humana. La supervisión permitirá detectar errores y cambios en el entorno donde operan los sistemas de IA, de forma de asegurar que los desarrollos estén al servicio de la persona humana. Asimismo, mediante esta obligación permite interpretar y contextualizar resultados entregados por un sistema de IA, mitigando posibles sesgos que puedan derivarse de su utilización.

Lo mismo puede decirse del sistema de gestión de riesgo que deben implementar

los sistemas de IA de alto riesgo, para garantizar que sean seguros, confiables y éticos. Por ello, los mecanismos de gestión de riesgos abordan la identificación, evaluación, mitigación y mejora continua de los sistemas de IA, apuntando, en último término, a generar confianza respecto de sus usos y aplicaciones.

En materia de gobernanza de datos, también se impone una obligación acorde al contexto de uso del sistema, exigencia derivada de la necesidad de que los datos se manejen de manera segura y se proteja la privacidad de las personas involucradas, cuando existan datos personales comprometidos. Del mismo modo, se genera una mayor transparencia y explicabilidad en el funcionamiento de estos sistemas, propiciando una definición clara de roles y responsabilidades en relación con la recopilación, el almacenamiento, el uso y el intercambio de dichos datos.

Por otro lado, para que este nuevo marco normativo opere con una estructura de gobernanza diversa, informada y legitimada, se ha estimado necesario contar con una instancia consultiva de carácter permanente. En este proyecto, la instancia asesora del Ministro o Ministra de CTCI será el Consejo Asesor Técnico de IA. Estará integrado por representantes del Estado, la academia, la industria de tecnología y la sociedad civil y funcionará ad-honorem, y abordará materias destinadas al desarrollo, promoción y mejoramiento continuo de los sistemas de IA en el país. En este sentido, se configurará como un organismo coadyuvante del Ministerio de CTCI.

6. Institucionalidad especializada

Con miras al resguardo de los derechos y libertades de las personas y la adecuada observancia de las prohibiciones

y reglas establecidas en la presente ley, se encomienda la labor de fiscalización y cumplimiento normativo a la Agencia encargada de la Protección de Datos Personales, cuya creación actualmente se tramita bajo el boletín N° 11.144-07.

La elección de la autoridad encargada de monitorear y eventualmente sancionar en aplicación de la normativa se efectúa considerando que la base de funcionamiento de cualquier sistema de IA es, precisamente, el uso de datos.

Asimismo, se propone el fortalecimiento del Ministerio CTCI en materia de IA. Para ello, se plantea la creación de un Departamento de tecnología e IA al interior de la división de políticas públicas del Ministerio CTCI. Este departamento será el encargado de articular el cumplimiento de los objetivos de trabajo del Consejo Asesor Técnico de IA e impulsar el desarrollo de políticas públicas en materia de IA. Se espera que pueda transformarse en una división dentro del Ministerio CTCI, con el objeto de consolidar estas capacidades al interior de la administración del Estado.

II. CONTENIDO

El presente proyecto de ley, que regula los sistemas de inteligencia artificial, consta de 31 artículos permanentes y 3 artículos transitorios, y se estructura sobre la base de los siguientes títulos: (a) Disposiciones generales, lo que comprende el ámbito de aplicación de la propuesta, definiciones y clasificación de los sistemas de IA; (b) Sistemas de riesgo inaceptable; (c) Sistemas de IA de alto riesgo; (d) Sistemas de IA de riesgo limitado; (e) Incidentes graves; (g) Gobernanza; (h) Medidas de apoyo a la innovación; (i) Confidencialidad, infracciones y sanciones; (j) Disposiciones finales y modificaciones a otros cuerpos legales.

1. Disposiciones generales

a. Ámbito de aplicación

El artículo 2° del proyecto de ley establece los sujetos pasivos de la ley, utilizando como factor de atribución la utilización de la información de salida del sistema de IA en Chile. Con ello, se busca asegurar la aplicación efectiva de esta normativa por la vía de identificar a un responsable del uso del sistema de IA en el territorio nacional.

Por su parte, el inciso segundo del artículo 2° exceptúa de la aplicación de la ley sobre determinados sistemas.

Adicionalmente, para efectos de precisar el ámbito de aplicación de la ley, dentro del artículo 3° se entregan una serie de definiciones sobre conceptos que cruzan el contenido y alcance de la norma. En este contexto, resulta de especial importancia la definición de “Sistemas de IA”.

b. Principios aplicables a sistemas de IA

Tratándose de los principios aplicables a los sistemas de IA, el artículo 4° plantea los principios generales a ser observados por los operadores. Entre ellos se encuentran:

- **Intervención y supervisión humana:** plantea que los sistemas de IA sean desarrollados y utilizados como una herramienta al servicio de las personas, que respete la dignidad humana y la autonomía personal, y que funcione de manera que pueda ser controlada y supervisada adecuadamente por seres humanos.
- **Solidez y seguridad técnica:** apunta a que los sistemas de IA sean desarrollados y utilizados de manera que se minimicen los daños previsibles en

contra de las personas, siendo técnicamente resistentes frente a fallas imprevistas como también frente a intentos de modificación del uso o rendimiento del sistema de IA con fines ilícitos por parte de terceros.

- **Privacidad y gobernanza de datos**: persigue que los sistemas de IA sean desarrollados y utilizados de conformidad con las normas vigentes en materia de privacidad y protección de datos personales, procurando que los mismos sean interoperables.
- **Transparencia y explicabilidad:** apunta a que los sistemas de IA sean transparentes en su funcionamiento y los procesos de toma de decisiones deben ser explicables. Esto implica que los usuarios deben poder entender cómo se llega a las conclusiones o recomendaciones de un sistema de IA.
- **Diversidad, no discriminación y equidad:** persigue que los sistemas de IA sean diseñados y utilizados durante todo su ciclo de vida, promoviendo la igualdad de oportunidades, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y sesgos de selección o de información que pudieran generar un efecto discriminatorio.
- **Bienestar social y medioambiental**: busca considerar y promover los impactos positivos en la sociedad y en el medio ambiente asociados al desarrollo, implementación y uso de sistemas de IA. Esto implica que los usos de esta tecnología se desarrollarán y utilizarán de manera sostenible y respetuosa con el medio ambiente y las personas, verificando los efectos a largo plazo que su aplicación genera en estos ámbitos.
- **Rendición de cuentas y responsabilidad:** apunta a que los sistemas de IA proporcionen un correcto funcionamiento a lo largo de todo su ciclo de vida por parte de quienes los diseñan,

desarrollan, operan o despliegan, en relación con sus funciones propias.

- **Protección de los derechos de los consumidores**: persigue que los sistemas de IA sean desarrollados y utilizados en línea con las normas vigentes en materia de protección de los derechos de los consumidores, debiendo asegurar un trato justo, entrega de información veraz, oportuna y transparente y el resguardo a la libertad de elección y la seguridad en el consumo de este tipo de tecnologías.

Los principios mencionados se implementarán en las distintas orientaciones que el Ministerio CTCI y la Agencia encargada de la Protección de Datos Personales pueda dar al respecto, en sus respectivas esferas de competencias.

c. Clasificación de los sistemas de IA

La clasificación de los sistemas de IA se recoge en el artículo 5° del proyecto de ley. De acuerdo al literal a) de este artículo, los sistemas de IA de riesgo inaceptable son aquellos incompatibles con el respeto y garantía de los derechos fundamentales de las personas. Por ello, se estiman contrarios al ordenamiento jurídico nacional y se prohíbe su uso conforme prescribe el artículo 6°.

Por su parte, el literal b) del artículo 5° define a los sistemas de IA de alto riesgo y el literal c) del artículo 5° define a los sistemas de IA de riesgo limitado como aquellos cuyo uso presenta riesgos de manipulación o engaño. El sistema de IA pueda arribar a resultados incorrectos o sesgados, con independencia

del mecanismo que se aplique. Por este motivo, se les imponen reglas de transparencia a este tipo de sistemas.

Finalmente, el artículo 5° letra d) define a aquellos sistemas de IA sin riesgo evidente.

7. Sistemas de IA de riesgo inaceptable

El artículo 6° de la presente iniciativa lista las categorías de sistemas de IA de riesgo inaceptable.

En particular, de acuerdo con los literales a) y b) del mencionado artículo, las prohibiciones comprenden las prácticas ya apuntadas con alto potencial para manipular a las personas.

Por su parte, la letra c) se refiere a los usos de sistemas de IA de categorización biométrica que estarán prohibidos. Excepcionalmente se permitirá en algunos casos el uso de este tipo de tecnologías para fines terapéuticos, en la medida que hayan sido autorizados sobre la base de un consentimiento informado específico y expreso de las personas expuestas a ellos, y se cuente además con la autorización sanitaria respectiva, en caso de ser procedente.

El artículo 6° literal d) de la propuesta prohíbe ciertos sistemas de IA de calificación social genérica.

En lo que concierne a los sistemas de IA basado en la identificación biométrica, el artículo 6° literal e) únicamente prohíbe la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para el análisis de imágenes de vídeo en espacios de acceso público que empleen sistemas de identificación biométrica remota en tiempo real. Con todo, esta prohibición no será aplicable en caso de que el sistema de IA sea utilizado por autoridades y órganos

encargados de la seguridad pública y organismos de persecución penal, con el objetivo de prevenir, investigar, detectar y, eventualmente, sancionar la comisión de crímenes o simples delitos o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública.

Por su parte, dentro del literal f) del artículo 6° de la presente propuesta se prohíbe la introducción en el mercado, puesta en servicio o utilización de sistemas de IA basados en técnicas de *facial scraping*, mediante la extracción no selectiva de imágenes faciales desde internet o de imágenes de circuitos cerrados de televisión.

Finalmente, el artículo 6° letra g) prohíbe aquellos sistemas de IA destinados a la evaluación de los estados emocionales de una persona en los ámbitos que allí se especifican.

8. Sistemas de IA de alto riesgo

El artículo 7° de la propuesta de ley caracteriza a los sistemas de alto riesgo. Se describen como aquellos que presentan un riesgo significativo de causar perjuicios para la salud, la seguridad, los derechos fundamentales protegidos por la Constitución Política de la República o el medioambiente, así como los derechos de los consumidores.

A diferencia de los sistemas de IA prohibidos se deja a un reglamento dictado por el Ministerio de CTCI la lista específica de sistemas de alto riesgo, que se elaborará previa propuesta efectuada por el Consejo Asesor Técnico de IA, conforme se establece en el artículo 15°.

En consonancia con un enfoque basado en riesgos, los sistemas de IA de alto riesgo están permitidos siempre que cumplan con una serie de reglas

obligatorias previstas dentro del artículo 8°.

a. Sistemas de gestión de riesgos

En cuanto al establecimiento de sistemas de gestión de riesgos, el artículo 8° literal a) establece que el mismo deberá basarse en un proceso iterativo continuo de evaluación de riesgos que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el que requerirá revisiones periódicas a fin de procurar su eficacia y minimizar que falle o funcione mal, en función de la finalidad prevista.

b. **Gobernanza de datos**

De acuerdo con el artículo 8° literal b), se establece que los sistemas de IA de alto riesgo que utilicen técnicas que impliquen el entrenamiento de modelos con datos, requerirán de una gobernanza de datos acorde al contexto del uso, así como a la finalidad prevista del sistema de IA, en la medida en que esto sea técnicamente posible.

c. Documentación técnica

El literal c) del artículo 8° prescribe que toda aquella documentación técnica que acompañe al sistema de IA de alto riesgo deberá será inteligible y se redactará de modo tal que demuestre que el sistema de IA de alto riesgo cumple con las reglas establecidas en la presente propuesta.

En la práctica, esta regla impondrá una medida de publicidad al operador que introduzca en el mercado o ponga en servicio un sistema de IA de alto riesgo, con el objeto de transparentar el funcionamiento técnico de dicha tecnología.

d. **Sistema de registros**

La regla relativa a la mantención de un sistema de registros, establecida en el artículo 8° literal d), prevé que los sistemas de IA de alto riesgo deberán diseñarse y desarrollarse con capacidades que permitan registrar información y eventos de seguridad mientras están en funcionamiento, las que además se ajustarán a las normas o especificaciones comunes reconocidas por el estado de la técnica.

e. Mecanismos de transparencia

El literal e) del artículo 8 prevé que los sistemas de IA de alto riesgo sean diseñados y desarrollados con un nivel de transparencia suficiente para que los operadores y sus destinatarios entiendan razonablemente su funcionamiento, con arreglo a su finalidad prevista.

Además, a partir del momento de la introducción en el mercado del sistema de IA de alto riesgo, se utilizarán todos los medios técnicos disponibles de conformidad con el estado actual de la técnica generalmente reconocido para posibilitar que los operadores puedan interpretar la información de salida del sistema de IA de alto riesgo.

Con esta regla se persigue facilitar la identificación y corrección de posibles errores o sesgos que podrían generar información de salida injusta o discriminatoria. Además, contribuye a asignar responsabilidades en caso de problemas éticos o legales vinculados al funcionamiento de un sistema de IA de alto riesgo, aumentando al mismo tiempo la confianza de los usuarios en la adopción y uso de este tipo de tecnologías.

f. Mecanismos de supervisión humana

En el literal f) del artículo 8 se establece que los sistemas de IA de alto riesgo deberán ser diseñados y desarrollados de modo tal que puedan ser supervisados por personas naturales técnicamente capacitadas para esta función según sea apropiado para el escenario de implementación en cuestión y de forma proporcionada a los riesgos asociados.

g. **Precisión, solidez y ciberseguridad**

Se plantea que los sistemas de IA de alto riesgo sean diseñados y desarrollados siguiendo el principio de seguridad desde el diseño y por defecto, debiendo contar con un nivel adecuado de precisión, solidez, seguridad y ciberseguridad y funcionar de manera consistente durante todo su ciclo de vida.

Asimismo, se establece como norma de clausura en el inciso final del artículo 8°, aplicable a todas las reglas relativas a los sistemas de IA de alto riesgo, la posibilidad de promover estándares diferenciados para el cumplimiento de las reglas indicadas precedentemente, tomando en consideración el tipo de operador y su tamaño, especialmente si se trata de empresas de menor tamaño.

El artículo 9° de la propuesta prevé que, en aquellos casos en que un sistema de IA de alto riesgo no se ajuste a las reglas aplicables a este tipo de sistemas, el operador adoptará inmediatamente las medidas necesarias para desactivarlo, retirarlo del mercado o recuperarlo.

El artículo 10° de la ley plantea el deber de los implementadores de establecer y documentar sistemas de seguimiento

posteriores a la comercialización de sistemas de alto riesgo.

9. Sistemas de IA de riesgo limitado

El artículo 11° de la propuesta de ley caracteriza a los sistemas de riesgo limitado como aquellos cuyo uso presenta un riesgo no significativo de manipulación, engaño o error, producto de su interacción con personas.

Por este motivo, la normativa propuesta persigue que los sistemas de IA de riesgo limitado procuren proveerse en condiciones transparentes, de modo tal que las personas sean informadas de forma clara y precisa, y les permitan estar conscientes de que están interactuando con una máquina.

Con todo, se establece una excepción a este deber de transparencia, tratándose de sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento penal.

10. Incidentes graves

El artículo 13° de la propuesta plantea que todo aquel que identifique un incidente grave -en los términos definidos dentro del artículo 3°- podrá reportarlo a la Agencia a cargo de la Protección de Datos Personales, quien informará al operador para que adopte las medidas de información y de respuesta frente a contingencias respectivas, tan pronto tome conocimiento del incidente.

De este modo, se prevé mitigar daños previstos e imprevistos, especialmente respecto de sistemas de IA de alto riesgo, y restaurar su funcionamiento normal.

11. Gobernanza en materia de IA

El proyecto de ley propone la siguiente gobernanza en materia de IA:

- **Creación del Consejo Asesor Técnico de IA (“Consejo Asesor de IA”)**: el artículo 14° de la propuesta plantea la creación del Consejo Asesor de IA y define su naturaleza.

  El artículo 15° señala las principales funciones del Consejo Asesor de IA. Entre ellas se encuentran (i) presentar al Ministro o Ministra CTCI una propuesta de listado de sistemas de IA de alto riesgo y de riesgo limitado, sobre la base de los criterios establecidos en la ley; (ii)asesorar a la Ministra o Ministro de CTCI respecto del alcance y modo de cumplimiento de las reglas a las que deberán sujetarse los operadores de sistemas de IA de alto riesgo y de riesgo limitado; y (iii) presentar a la Ministra o Ministro de CTCI una propuesta relativa al establecimiento de los lineamientos para el desarrollo de espacios controlados de prueba para los sistemas de IA, así como para la fijación de estándares mínimos de cumplimiento y rendición de cuentas para su desarrollo.

  Por último, los artículos 16° a 18° regulan aspectos relativos a las inhabilidades para integrar esta entidad, causales de cesación en el cargo de consejeros o consejeras y otras normas de funcionamiento.

- **Fiscalización y cumplimiento a cargo de la Agencia encargada de la protección de datos personales (“Agencia”)**: Dentro de las funciones de la Agencia se encuentran: (i) fiscalizar el cumplimiento de las disposiciones de esta ley y su reglamento; (ii) Determinar las infracciones e incumplimientos en que incurran quienes contravengan las prohibiciones o no cumplan las obligaciones de la presente ley; (iii) Ejercer la potestad sancionadora sobre las personas

naturales o jurídicas que contravengan las disposiciones de la presente ley y su reglamento; (iv) Resolver las solicitudes y reclamos que formulen las personas afectadas contra quienes contravengan las prohibiciones o no cumplan las obligaciones de la presente ley y su reglamento.

12. Medidas de apoyo a la innovación

En el título VII, entre los artículos 20 y 22, se plantean las medidas de apoyo a la innovación ya comentadas, respecto a espacios controlados de pruebas y aquellas dirigidas a empresas de menor tamaño.

13. Confidencialidad, infracciones y sanciones

El artículo 23° establece normas de resguardo de la confidencialidad de la información y los datos obtenidos de un sistema de IA en el ejercicio de sus funciones y actividades.

Por su parte, en lo referente a infracciones y sanciones, los artículos 24° al 27° establecen el catálogo de infracciones y sanciones administrativas aplicables por parte de la Agencia en caso de incumplimiento de las prohibiciones y obligaciones establecidas en la ley, además de las reglas a las que se sujetará el procedimiento administrativo sancionador y el de reclamación judicial que pueda originarse como consecuencia de la imposición de una sanción administrativa.

Finalmente, los artículos 28° y 29° regulan la acción de responsabilidad civil por culpa que podría derivarse de la generación de un daño provocado por la utilización de un sistema de IA, así como su procedimiento aplicable.

14. Disposiciones finales, modificación a otros cuerpos legales y disposiciones transitorias

En materia de disposiciones finales, el artículo 30° dispone que un reglamento dictado por intermedio del Ministerio CTCI establecerá el listado de sistemas de IA de alto riesgo y de sistemas de IA de riesgo limitado respecto de los cuales serán aplicables las reglas establecidas para cada uno de ellos, así como el contenido mínimo y forma de dar cumplimiento a dichas reglas.

Con respecto a las modificaciones a otras normas, el artículo 30° plantea una modificación a la ley N°17.336 de propiedad intelectual, incorporando una nueva excepción en materia de derechos de autor que permite la extracción, comparación, clasificación, o cualquier otro análisis estadístico de datos de lenguaje, sonido o imagen, o de otros elementos de los que se componen por grandes volúmenes de datos u obras, en la medida que dicho uso no constituya una explotación encubierta de obras protegidas por derechos de autor. Con ello se permite modernizar la normativa vigente, en línea con los procesos de análisis y minería de grandes volúmenes de datos, propios del entrenamiento de sistemas de IA.

Por último, las disposiciones transitorias plantean, por un lado, la fecha de entrada en vigor de la presente ley y los plazos dentro de los cuales deberán dictarse las normas y actos administrativos necesarios para su plena vigencia.

En mérito de lo anteriormente expuesto, someto a vuestra consideración el siguiente

REPUBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

P R O Y E C T O D E L E Y :

“TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto de la ley. La presente ley tiene por objeto promover la creación, desarrollo, innovación e implementación de sistemas de inteligencia artificial (“IA”) al servicio del ser humano, que sean respetuosos de los principios democráticos, el Estado de Derecho y los derechos fundamentales de las personas frente a los efectos nocivos que determinados usos pudieran irrogar.

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

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

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

c) 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.

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

Con todo, la presente ley no será aplicable a:

a) 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 inciso precedente.

b) Las actividades de investigación, pruebas y desarrollo sobre sistemas de IA de forma previa a su introducción en el mercado o puesta en servicio, siempre que dichas actividades se lleven a cabo respetando los derechos fundamentales de las personas. Si se producen daños con ocasión de dichas actividades se responderá de acuerdo con las normas de los artículos 21 y 28 de la presente ley.

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 las normas del artículo 28 de la presente ley.

Artículo 3.- Definiciones. Para los efectos de la presente ley, se entenderá por:

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

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

3. **Riesgo significativo**: riesgo que resulta como consecuencia 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.

4. **Proveedor**: toda persona natural o jurídica u organismo del Estado que desarrolle un sistema de IA con miras a introducirlo en el mercado o ponerlo en servicio, a título gratuito u oneroso.

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

6. **Proveedor de tecnología**: todo proveedor involucrado con el implementador en la comercialización y suministro de *softwares*, herramientas y componentes de *softwares*, modelos y datos previamente entrenados.

7. **Representante autorizado**: toda persona natural o jurídica domiciliada en Chile que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA para cumplir con las obligaciones establecidas en la presente ley en representación de dicho proveedor.

8. **Importador**: toda persona natural o jurídica domiciliada en Chile que introduzca en el mercado o ponga 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**: toda persona natural o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice 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 el distribuidor.

11. **Persona afectada**: toda persona natural o grupo de personas naturales expuesta a un sistema de IA que sufra un perjuicio como consecuencia de dicha exposición.

12. **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.

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

14. **Verificación biométrica**: la verificación automatizada de la identidad de una persona mediante la comparación de sus datos biométricos con los datos biométricos proporcionados con anterioridad, que incluye la autenticación.

15. **Sistema de identificación biométrica remota**: un sistema de IA destinado a identificar a personas naturales a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el

implementador del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada.

16. **Sistema de identificación biométrica remota "en tiempo real":** un sistema de identificación biométrica remota en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa.

17. **Sistema de reconocimiento de emociones**: un 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 sus datos de base biométrica.

18. **Incidente grave**: todo incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga, pueda haber tenido o pueda tener alguna de las siguientes consecuencias:

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

b) Una alteración grave de la gestión y el funcionamiento de infraestructura crítica, entendida en los términos del artículo 32 N°21 inciso segundo de la Constitución Política de la República.

c) Una vulneración de derechos fundamentales protegidos en virtud de la Constitución y las leyes.

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

19. **Elaboración de perfiles**: toda forma de tratamiento automatizado de datos personales sensibles consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona natural, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

20. **Espacio controlado de pruebas**: un entorno controlado creado por un órgano de la administración del Estado y que facilita el desarrollo, la prueba y la validación de sistemas de IA innovadores durante un período limitado

antes de su introducción en el mercado o su puesta en servicio, con arreglo a un plan específico diseñado por éste.

21. **Espacio de acceso público: cualquier lugar físico de** propiedad pública o privada que sea accesible para el público, con independencia de que deban cumplirse determinadas condiciones para acceder a él y con independencia de posibles restricciones de aforo.

22. **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 puedan inferirse a partir de dichos datos.

23. **Componente de seguridad de un producto o sistema**: un componente de un producto o un sistema de IA que cumple una función de seguridad para dicho producto o sistema, o cuya falla o defecto de funcionamiento pone en peligro la salud y la seguridad de las personas.

24. **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 una interacción con otros sistemas (incluidos otros sistemas de IA) razonablemente previsible.

25. **Finalidad prevista**: el uso para el que un proveedor concibe un sistema de IA, incluido el contexto y las condiciones de uso concretas, según la información facilitada por el proveedor 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 que entren en el ámbito de aplicación de la presente ley deberán observar los siguientes principios generales:

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

b) **Solidez y seguridad técnica**: los sistemas de IA se desarrollarán y utilizarán de manera que se minimicen los daños previsibles, siendo 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.

c) **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, y sólo tratarán datos que cumplan con la normativa en términos de calidad e integridad. Del mismo modo, se procurará que los datos que utilicen sean interoperables.

d) **Transparencia y explicabilidad**: los sistemas de IA se desarrollarán y utilizarán facilitando una trazabilidad y explicabilidad adecuadas, de modo tal que los seres humanos puedan conocer de forma clara y precisa y sean conscientes de que se comunican o interactúan con un sistema de IA, en aquellos casos en los que dicho conocimiento les ayudaría a tomar decisiones sobre sus derechos, seguridad o privacidad, informando a sus destinatarios, cuando corresponda, cómo el sistema ha obtenido sus predicciones o resultados, así como también sobre las capacidades y limitaciones de dicho sistema de IA.

e) **Diversidad, no discriminación y equidad**: los sistemas de IA se desarrollarán y utilizarán durante todo su ciclo de vida, promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y sesgos de selección o de información que pudieran generar un efecto discriminatorio.

f) **Bienestar social y medioambiental**: los sistemas de IA se desarrollarán y utilizarán de manera sostenible y respetuosa con el medio ambiente y los seres humanos. 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.

g) **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.

h) **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, debiendo 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.

El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación y la Agencia encargada de la Protección de Datos Personales, en adelante "la Agencia", 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 dentro de 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.

Artículo 5.- Clasificación de los sistemas de IA. Los usos de los sistemas de IA se clasificarán, de acuerdo con su riesgo, en las siguientes categorías:

a) Sistemas de IA de riesgo inaceptable: Agrupa a sistemas de IA incompatibles con el respeto y garantía de los derechos fundamentales de las personas, por lo que su introducción en el mercado o puesta en servicio se encuentra prohibida.

b) Sistemas de IA de alto riesgo: Agrupa a sistemas de IA autónomos o componentes de seguridad de productos que pueden afectar negativamente a la salud y la seguridad de las personas, sus derechos fundamentales o el medio ambiente, así como los derechos de los consumidores, especialmente si fallan o se utilizan de forma impropia.

c) Sistemas de IA de riesgo limitado: Agrupa a sistemas de IA que presentan riesgos no significativos de manipulación, engaño o error, producto de su interacción con personas naturales.

d) Sistemas de IA sin riesgo evidente: Agrupa a todos los demás sistemas de IA que no entran en las categorías mencionadas en los literales precedentes.

TÍTULO II

SISTEMAS DE INTELIGENCIA ARTIFICIAL DE RIESGO INACEPTABLE

Artículo 6.- Sistemas de IA de riesgo inaceptable. Serán sistemas de IA de riesgo inaceptable aquellos que queden comprendidos en algunas de las siguientes categorías:

a) **Sistemas de manipulación subliminal**: sistemas de IA que se sirven de técnicas imperceptibles para las personas afectadas y que tienen como objeto o efecto directo la inducción de acciones que causan daños a la salud física y/o mental de la persona afectada.

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 de las personas expuestas a ellos o, en su caso, de su representante legal o judicial, además de la autorización sanitaria respectiva, de ser procedente.

b) **Sistemas que explotan vulnerabilidades de las personas para generar comportamientos dañinos**: sistemas de IA que aprovechan o explotan alguna de las vulnerabilidades de una persona o un grupo específico de personas —incluidas las características conocidas de los rasgos de personalidad, situación social o económica de esa persona o grupo, la edad y la capacidad física o mental— que tenga por objeto alterar de manera sustancial su comportamiento o limitar su voluntad y provoque perjuicios, actuales o potenciales, a esa persona o a terceros.

Asimismo, se entenderán incluidos dentro de esta categoría aquellos sistemas de IA que sean dañinos y/o afecten la honra, la integridad y el libre desarrollo de la sexualidad de las personas, en particular la de niños, niñas y adolescentes.

c) **Sistemas de categorización biométrica de personas basadas en datos personales sensibles**: sistemas de categorización biométrica que clasifiquen e identifiquen a personas naturales con arreglo a datos personales sensibles, o que partan de la base de una inferencia respecto a dichos atributos o características, de modo tal que dicha categorización provoque un trato perjudicial o injustificadamente discriminatorio sobre ellas.

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, de las personas naturales expuestas a ellos o, en su caso, de su representante legal o judicial, además de la autorización sanitaria respectiva, de ser procedente.

d) **Sistemas de 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 un trato perjudicial o injustificadamente discriminatorio sobre dichas personas o grupos de personas.

e) **Sistemas de identificación biométrica remota en espacios de acceso público en tiempo real**: sistemas de IA destinados al análisis de imágenes de vídeo en espacios de acceso público que emplean sistemas de identificación biométrica remota en tiempo real.

Esta prohibición no será aplicable, en caso de que el sistema de IA sea utilizado estrictamente por las autoridades y órganos encargados de la seguridad pública y organismos de persecución penal, con el objetivo de prevenir, investigar, detectar y, eventualmente, sancionar la comisión de crímenes o simples delitos o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, de conformidad con la ley.

f) **Sistemas de extracción no selectiva de imágenes faciales** sistemas de IA que crean o amplían bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales a partir de internet o de imágenes de circuito cerrado de televisión.

g) **Sistemas de evaluación de los estados emocionales de una persona**: sistemas de IA que infieren las emociones de una persona natural en los ámbitos de la aplicación de la ley penal, procesal penal y la gestión de fronteras, en lugares de trabajo y en centros educativos.

TÍTULO III

SISTEMAS DE IA DE ALTO RIESGO

Artículo 7.- Sistemas de IA de alto riesgo. Un sistema de IA se considerará de alto riesgo cuando presente un riesgo significativo de causar perjuicios para la salud, la seguridad, los derechos fundamentales protegidos por la Constitución Política de la República o el medioambiente, así como los derechos de los consumidores, con independencia de si se ha introducido en el mercado o se ha puesto en servicio, 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.

Los sistemas de IA de alto riesgo deberán procurar el respeto de los derechos fundamentales de las personas afectadas por el sistema. 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 8.- Reglas aplicables a los sistemas de IA de alto riesgo. Los sistemas de IA de alto riesgo deberán cumplir con las siguientes reglas relativas a:

a) **Establecimiento de sistemas de gestión de riesgos**: Los sistemas de IA de alto riesgo se someterán a un proceso iterativo continuo de evaluación de riesgos que se llevará a cabo durante todo el ciclo de vida de del sistema, el cual requerirá revisiones y actualizaciones periódicas a fin de procurar su eficacia y minimizar las posibilidades de que falle o funcione mal, en función de la finalidad prevista declarada.

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

b) **Gobernanza de datos**: Los sistemas de IA de alto riesgo que utilicen técnicas que impliquen el entrenamiento de modelos con datos estarán sometidos a una gobernanza de datos acorde al contexto del uso, así como a la finalidad prevista del sistema de IA, en la medida en que esto sea técnicamente posible de conformidad con el segmento de mercado o ámbito de aplicación de que se trate. Asimismo, deberán procurar incorporar estándares técnicos y de seguridad de datos aceptados internacionalmente.

c) **Documentación técnica**: La documentación técnica que acompañe al sistema de IA de alto riesgo será inteligible y se redactará de modo tal que demuestre que el sistema de IA de alto riesgo cumple con las reglas establecidas en la presente ley.

d) **Sistema de registros**: Los sistemas de IA de alto riesgo se diseñarán y desarrollarán con capacidades que permitan registrar información y eventos de seguridad mientras están en funcionamiento. Estas capacidades de registro se ajustarán a las normas o las especificaciones comunes reconocidas y al estado de la técnica.

e) **Mecanismos de transparencia**: Los sistemas de IA de alto riesgo se diseñarán y desarrollarán con un nivel de transparencia suficiente para que los operadores y sus destinatarios entiendan razonablemente el funcionamiento del sistema, con arreglo a su finalidad prevista.

En el momento de la introducción en el mercado del sistema de IA de alto riesgo, se utilizarán todos los medios técnicos disponibles de conformidad con el estado actual de la técnica generalmente reconocido para posibilitar que los operadores puedan interpretar la información de salida del sistema de IA de alto riesgo.

f) **Mecanismos de supervisión humana**: Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser supervisados por personas naturales técnicamente capacitadas para esta función según sea apropiado para el escenario de implementación en cuestión y de forma proporcionada a los riesgos asociados, con el objeto de prevenir o reducir al mínimo los riesgos para la salud, la seguridad, los derechos fundamentales, la democracia, y/o el medio ambiente, que puedan surgir cuando un sistema de IA de alto riesgo se utilice conforme a su finalidad prevista o cuando se le dé un uso indebido razonablemente previsible.

g) **Precisión, solidez y ciberseguridad**: Los sistemas de IA de alto riesgo se diseñarán y desarrollarán siguiendo el principio de seguridad desde el diseño y por defecto, debiendo contar con un nivel adecuado de precisión, solidez, seguridad y ciberseguridad, funcionando de manera consistente, confiable y robusta durante todo su ciclo de vida. El cumplimiento de estos requisitos debe estar vinculado a la aplicación de medidas conformes al estado de la técnica, de acuerdo con el segmento de mercado o ámbito de aplicación específicos.

En cualquier caso, para el cumplimiento de las reglas precedentes, se podrán establecer estándares diferenciados en virtud del tipo de operador y en consideración a su tamaño, especialmente teniendo en consideración 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.

Artículo 9.- Medidas frente a contingencias. Cuando un sistema de IA de alto riesgo introducido en el mercado o puesto en servicio no se ajuste a las reglas previstas en la presente ley, el operador, asistido por su proveedor de tecnología, cuando sea procedente, adoptará inmediatamente las

medidas necesarias para desactivarlo, retirarlo del mercado o recuperarlo.

Estas medidas se encontrarán establecidas dentro del sistema de gestión de riesgos del respectivo sistema de IA de alto riesgo y serán diseñadas de conformidad con su finalidad de uso.

Artículo 10.- Seguimiento posterior a la comercialización para sistemas de IA de alto riesgo. Los implementadores establecerán y documentarán un sistema de seguimiento posterior a la comercialización que sea proporcional a la naturaleza y riesgos identificados de los sistemas de IA de alto riesgo.

El sistema de seguimiento posterior a la comercialización recabará y analizará datos proporcionados por implementadores o recopilados a través de otras fuentes, sobre el funcionamiento de los sistemas de IA de alto riesgo durante toda su vida útil, y permitirá a los operadores determinar el nivel de cumplimiento de las reglas del artículo 8 de la presente ley.

Cuando proceda, el seguimiento posterior a la comercialización incluirá un análisis de la interacción con otros entornos de sistemas de IA, incluidos otros dispositivos y software.

TÍTULO IV

SISTEMAS DE IA DE RIESGO LIMITADO

Artículo 11.- Sistemas de IA de riesgo limitado. Un sistema de IA se considerará de riesgo limitado cuando su uso presente un riesgo no significativo de manipulación, engaño o error, producto de su interacción con personas naturales.

Los sistemas de IA de riesgo limitado deberán procurar proveerse en condiciones transparentes, de modo tal que las personas sean informadas de forma clara y precisa, y les permitan estar conscientes de que están interactuando con una máquina.

Artículo 12.- Obligaciones de transparencia en sistemas de IA de riesgo limitado. Los proveedores e implementadores procurarán que los sistemas de IA de riesgo limitado estén diseñados y desarrollados de forma que el sistema de IA, el propio proveedor o el usuario informen de manera clara, inteligible y oportuna a dichas personas naturales expuestas a un sistema de IA de que están interactuando con un sistema de IA, excepto en las situaciones en las que esto resulte

evidente debido a las circunstancias y al contexto de utilización.

Con todo, este deber no se aplicará a los sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento penal, salvo que estos sistemas estén a disposición del público para denunciar ilícitos de carácter penal.

TÍTULO V

INCIDENTES GRAVES

Artículo 13.- Incidentes graves. Todo aquel que identifique un incidente grave, en los términos del numeral 18 del artículo 3 de la presente ley, podrá reportarlo a la Agencia encargada de la Protección de Datos Personales, quien, en el ámbito de sus competencias, informará de esta circunstancia al operador con miras a que éste pueda notificar a las personas afectadas por el incidente grave y, asimismo, adopte las medidas frente a contingencias correspondientes. Dicha notificación se efectuará tan pronto tome conocimiento del incidente, después de que el proveedor o, en su caso, el implementador haya establecido un vínculo causal entre el sistema de IA y el incidente, o la posibilidad razonable de que exista dicho vínculo, y, en cualquier caso, a más tardar setenta y dos horas después de que el proveedor o, en su caso, el implementador tenga conocimiento de dicho incidente grave.

Una vez que hayan establecido un vínculo causal entre el sistema de IA y el incidente grave, o la posibilidad razonable de que exista dicho vínculo, el operador adoptará las medidas oportunas de conformidad con el artículo 9 de la presente ley.

TÍTULO VI

GOBERNANZA

Artículo 14.- Consejo Asesor Técnico de Inteligencia Artificial. Créase el Consejo Asesor Técnico de Inteligencia Artificial (el “Consejo Asesor de IA”) como una instancia de carácter consultiva y permanente que asesorará al Ministro o Ministra de Ciencia, Tecnología, Conocimiento e Innovación en materias vinculadas al desarrollo, promoción y mejoramiento continuo de los sistemas de IA en el país.

El Consejo Asesor de IA será presidido por la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e

Innovación o la funcionaria o funcionario que designe al efecto y será integrado por:

a) Un representante del Ministerio encargado de la seguridad pública.

b) Un representante del Ministerio de Relaciones Exteriores.

c) Un representante del Ministerio de Defensa Nacional.

d) Un representante de la Secretaría de Gobierno Digital del Ministerio de Hacienda.

e) Un representante del Ministerio de Economía, Fomento y Turismo.

f) Un representante de la Subsecretaría de Telecomunicaciones.

g) Un representante de la Agencia encargada de la Protección de Datos Personales.

h) Un representante de la Agencia Nacional de Ciberseguridad.

i) Un académico experto en derecho y tecnología.

j) Un académico experto en sistemas de inteligencia artificial y/o ciencia de datos.

k) Un académico experto en ciberseguridad y/o en protección de datos personales.

l) Dos representantes de la industria de tecnología.

m) Dos representantes de organizaciones de la sociedad civil.

Los integrantes indicados en los literales a), b), c), d), e), f), g) y h) serán nombrados por el respectivo ministro o ministra de Estado, subsecretario o subsecretaria o jefe o jefa superior del servicio público, según fuere el caso. Por su parte, los integrantes mencionados en los literales i), j), k), l) y m) serán nombrados por la Ministra o el Ministro de Ciencia, Tecnología, Conocimiento e Innovación y durarán 2 años en sus cargos.

Artículo 15.- Funciones del Consejo Asesor de IA: Serán funciones del Consejo Asesor de IA, las siguientes:

a) Presentar a la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación una propuesta de listado de sistemas de IA de alto riesgo y de riesgo limitado, para la elaboración del reglamento al que se refiere el artículo 30 de la presente ley. En todo caso, dicho listado será elaborado sobre la base de los criterios establecidos en la presente ley y será actualizado, al menos, cada dos años.

b) Asesorar a la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación respecto del alcance y modo de cumplimiento de las reglas a las que deberán sujetarse los operadores de sistemas de IA de alto riesgo y de riesgo limitado.

c) Presentar a la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación una propuesta relativa al establecimiento de los lineamientos para el desarrollo de espacios controlados de prueba para los sistemas de IA, así como para la fijación de estándares mínimos de cumplimiento y rendición de cuentas para su desarrollo.

Los miembros del Consejo Asesor de IA no percibirán dieta por el desempeño de sus funciones.

La Subsecretaría de Ciencia, Tecnología, Conocimiento e Innovación proporcionará al Consejo Asesor de IA el apoyo administrativo y los recursos necesarios para el cumplimiento de sus funciones.

Artículo 16.- Inhabilidades. No podrán ser designados ni desempeñarse como miembros del Consejo Asesor de IA:

1. Las personas que hubieren sido condenadas por delito que merezca la pena aflictiva o inhabilitación perpetua para desempeñar cargos y oficios públicos, quienes hubieren sido condenados por violencia intrafamiliar constitutiva de delito conforme a la ley N°20.066 y, en general, quienes se encuentren inhabilitados para el ejercicio de la función pública de conformidad con el literal f) del artículo 12 de la ley Nº 18.834, sobre Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2004, del Ministerio de Hacienda.

2. Las personas que hubieren cesado en un cargo público como consecuencia de haber obtenido una calificación deficiente o por medida disciplinaria.

3. Las personas que tuvieren dependencia de sustancias o drogas estupefacientes o sicotrópicas cuya venta no se encuentre autorizada por la ley, a menos que se justifique su consumo por un tratamiento médico.

Si alguno de los miembros del Consejo Asesor de IA hubiere sido acusado de alguno de los delitos señalados en el numeral 1, quedará suspendido de su cargo hasta que concluya el proceso por sentencia firme.

Artículo 17.- Causales de cesación. Serán causales de cesación en el cargo, las siguientes:

1. Expiración del plazo señalado en el artículo 14.
2. Renuncia.
3. Sobreviniencia de alguna causal de inhabilidad contemplada en el artículo 16, la que será declarada en virtud de resolución dictada por la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación.

Artículo 18.- Normas de funcionamiento. El Consejo Asesor de IA sesionará con la asistencia de al menos nueve de sus miembros, y deberá adoptar sus acuerdos con el voto favorable de la mayoría de los asistentes. En caso de empate, dirimirá quien presida la reunión.

El Consejo Asesor de IA establecerá sus demás normas de funcionamiento interno, las que serán aprobadas por tres cuartos de sus miembros en ejercicio, y su aprobación se dispondrá mediante decreto supremo expedido a través del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación.

Artículo 19.- Fiscalización y cumplimiento. La fiscalización y el cumplimiento de las disposiciones de esta ley y su reglamento corresponderá a la Agencia . En particular, sus funciones serán:

a) Fiscalizar el cumplimiento de las disposiciones de esta ley y su reglamento. Para ello, podrá requerir a cualquier operador la entrega de toda la información que fuere necesaria para el cumplimiento de su función fiscalizadora.

b) Determinar las infracciones e incumplimientos en que incurran quienes contravengan las prohibiciones o no cumplan las obligaciones de la presente ley. Para tales efectos, podrá citar a declarar al operador, sus representantes legales, administradores, asesores y dependientes, así como a toda persona que haya tenido

participación o conocimiento respecto de algún hecho que sea relevante para resolver un procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones respectivas por otros medios que aseguren su fidelidad.

c) Ejercer la potestad sancionadora sobre las personas naturales o jurídicas que contravengan las disposiciones de la presente ley y su reglamento, aplicando las sanciones establecidas en el artículo 24.

d) Resolver las solicitudes y reclamos que formulen las personas afectadas contra quienes contravengan las prohibiciones o no cumplan las obligaciones de la presente ley y su reglamento.

TÍTULO VII

MEDIDAS DE APOYO A LA INNOVACIÓN

Artículo 20.- Espacios controlados de pruebas para la IA. Los órganos de la administración del Estado podrán proporcionar un espacio controlado que fomente la innovación y facilite el desarrollo, la prueba y la validación de sistemas innovadores de IA en la esfera de sus competencias, durante un período limitado antes de su introducción en el mercado o su puesta en servicio, con arreglo a un plan específico acordado entre los proveedores potenciales y las autoridades creadoras de tales espacios.

Los órganos de la administración del Estado que decidan crear espacios controlados de pruebas proporcionarán orientación y supervisión con miras a detectar riesgos significativos sobre los derechos fundamentales de las personas asegurados por la Constitución Política de la República, la salud, la seguridad, la democracia, o el medio ambiente, así como también para probar y demostrar la eficacia de las medidas de mitigación propuestas.

Todo riesgo significativo para los derechos fundamentales, la salud, la seguridad, la democracia, o el medio ambiente que sea detectado durante el proceso de desarrollo y prueba de estos sistemas de IA, implicará un deber de mitigación inmediato y apropiado por parte del operador que participe en el espacio controlado de prueba. Los órganos de la administración del Estado involucrados estarán facultados para suspender temporal o permanentemente el proceso de prueba si no se logra mitigar el riesgo significativo detectado.

Artículo 21.- Responsabilidad generada a partir de espacios controlados de pruebas para la IA. Los proveedores potenciales 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 y cuando los proveedores potenciales respeten el plan específico a que se refiere el inciso primero del artículo precedente y sigan de buena fe la orientación proporcionada por los órganos de la administración del Estado, estarán exentos del pago de las multas administrativas a las que se refiere el artículo 25 de la presente ley, sin perjuicio de la responsabilidad por los daños que pudieren causar.

Articulo 22.- Medidas dirigidas a empresas de menor tamaño. El Estado, a través de los ministerios de Ciencia, Tecnología, Conocimiento e Innovación y de Economía, Fomento y Turismo, propiciará medidas tendientes a:

a) 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,

b) 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.

c) Fomentar la participación de representantes de empresas de menor tamaño en el Consejo Asesor Técnico de IA, mediante la solicitud de opiniones al Consejo Consultivo de la Empresa de Menor Tamaño, previsto en la ley N°20.416 que fija normas especiales para las empresas de menor tamaño, dentro de la esfera de sus competencias.

TÍTULO VIII

CONFIDENCIALIDAD, INFRACCIONES Y SANCIONES

Artículo 23.- Confidencialidad. Toda persona natural, jurídica u órgano de la administración del Estado involucrado en la aplicación de la presente ley deberá 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:

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

b) Los datos personales y su tratamiento de conformidad con la normativa vigente;

c) El interés público y la seguridad nacional; y

d) La integridad de las causas penales o los procedimientos administrativos.

Artículo 24.- Infracciones. Para efectos del ejercicio de las atribuciones de la Agencia encargada de la Protección de Datos Personales, se considerará como infracción:

a) Gravísima: La puesta en servicio o la utilización de un sistema de IA de riesgo inaceptable a las que se refiere el artículo 6.

b) Grave: el incumplimiento de las reglas dispuestas en el artículo 8 para los sistemas de IA de alto riesgo.

c) Leve: el incumplimiento de las obligaciones de transparencia dispuestas respecto de los sistemas de IA de riesgo limitado del artículo 11.

Artículo 25.- Sanciones. La infracción a los preceptos de esta ley será sancionada de la siguiente manera:

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

b) Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales.

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

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

1. La duración de la infracción y sus consecuencias, considerando el propósito del sistema de IA,

así como, cuando proceda, el número de particulares afectados y el nivel de los daños ocasionados.

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

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

4. El grado de cooperación con las autoridades nacionales competentes con el fin de poner remedio a la infracción y mitigar sus posibles efectos adversos.

Artículo 26.- Procedimiento administrativo sancionador. La determinación de las infracciones que cometa un operador por vulnerar las prohibiciones o las obligaciones establecidas en esta ley y la aplicación de las sanciones correspondientes se sujetará a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Agencia.

b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o por denuncia. Junto con la apertura del expediente, la Agencia deberá designar un funcionario responsable de la instrucción del procedimiento.

c) La Agencia deberá presentar una formulación de cargos en contra del operador en que describa los hechos que configuran la infracción, los incumplimientos o infracciones detectadas, las normas infringidas y cualquier otro antecedente que sirva para sustentar la formulación.

d) La formulación de cargos debe notificarse al operador a su domicilio postal o a su dirección de correo electrónico.

e) El operador tendrá un plazo de quince días hábiles para presentar sus descargos. En esa oportunidad, podrá acompañar todos los antecedentes de hecho y de derecho que estime pertinentes para desacreditar los hechos imputados o que permitan desestimar total o parcialmente su responsabilidad. Junto con los descargos, el operador deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones.

f) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia podrá abrir un término probatorio de diez días en el caso que existan hechos sustanciales, pertinentes y controvertidos.

g) La Agencia dará lugar a las medidas o diligencias probatorias que solicite el operador en sus descargos, siempre que sean pertinentes y necesarias. En caso de rechazo, deberá fundar su resolución.

h) Los hechos investigados y las responsabilidades de los presuntos infractores pueden acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

i) La Agencia tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

j) La resolución que ponga fin al procedimiento sancionatorio debe ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por el operador y contendrá la declaración de haberse configurado la infracción a las prohibiciones o el incumplimiento de las obligaciones establecidas en la ley por el operador, según corresponda.

k) En caso de que la Agencia considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.

l) La resolución que establezca la infracción a las prohibiciones o el incumplimiento de las obligaciones establecidas en la ley y aplique la sanción correspondiente deberá ser fundada. Esta resolución deberá indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable judicialmente conforme al artículo siguiente.

m) El procedimiento administrativo de infracción de ley no podrá superar los seis meses.

Artículo 27.- Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones del lugar donde se encuentre domiciliado el reclamante. El reclamo deberá interponerse dentro de los quince días siguientes a la notificación de la resolución impugnada, los que deberán computarse de acuerdo con el artículo 25 de la ley N° 19.880, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le causa agravio.

b) La Corte podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior. Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado pueda ocasionar un daño irreparable al recurrente.

c) Recibida la reclamación, la Corte requerirá el informe de la Agencia, concediéndole un plazo de diez días hábiles al efecto.

d) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

e) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

f) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, cuando sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

g) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá rechazar o acoger la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda, y mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso.

h) Contra la resolución de la Corte de Apelaciones se podrá recurrir ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta.

i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.

Artículo 28.- Responsabilidad civil. La persona que sufra un daño como consecuencia de la utilización de un sistema de IA, podrá demandar civilmente y de forma conjunta respecto del operador:

a) La cesación de los actos generadores de daño.

b) La indemnización de los daños y perjuicios.

c) La adopción de las medidas necesarias para evitar que prosiga la infracción.

d) 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.

Artículo 29.- Procedimiento aplicable en materia civil. La acción civil establecida en el artículo 28 se tramitará conforme al procedimiento sumario, de conformidad a las disposiciones del título XI del libro III del Código de Procedimiento Civil.

TÍTULO IX
DISPOSICIONES FINALES

Artículo 30.- Reglamento. Un reglamento dictado por intermedio del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación establecerá el listado de sistemas de IA de alto riesgo y de sistemas de IA de riesgo limitado respecto de los cuales serán aplicables las reglas de los artículos 8 y 11, respectivamente.

El reglamento especificará, adicionalmente, lo siguiente:

- El contenido mínimo y forma de dar cumplimiento a las reglas aplicables a los sistemas de IA de alto riesgo del artículo 8.

- Los tipos de medidas frente a contingencias aplicables a los sistemas de IA de alto riesgo, en función de la finalidad del sistema de IA de alto riesgo.

- El contenido mínimo y forma de dar cumplimiento a las reglas aplicables a los sistemas de IA de riesgo limitado del artículo 10.

TÍTULO X
MODIFICACIONES A OTROS CUERPOS LEGALES

Artículo 31.- Incorpórase en la ley N° 17.336 sobre Propiedad Intelectual el siguiente artículo 71 T, nuevo:

"Artículo 71 T.- Es lícito, sin remunerar ni obtener autorización del titular, todo acto de reproducción, adaptación, distribución o comunicación al público, de una obra lícitamente publicada, cuando dicho acto se realice exclusivamente para la extracción, comparación, clasificación, o cualquier otro análisis estadístico de datos de lenguaje, sonido o imagen, o de otros elementos de los que se componen un gran número de obras o un gran volumen de datos, siempre que dicha utilización no constituya una explotación encubierta de la obra o de las obras protegidas.".

DISPOSICIONES TRANSITORIAS

Artículo primero.- Las normas de la presente ley entrarán en vigencia el primer día hábil del año siguiente a su publicación en el Diario Oficial.

Artículo segundo.- El decreto supremo que fija las normas de funcionamiento del Consejo Asesor Técnico de IA al que se refiere el artículo 18 de la presente ley, deberá dictarse dentro de un plazo de 6 meses contados desde la publicación de la presente ley en el Diario Oficial.

Las normas relativas a la aplicación del reglamento del artículo 25 de la presente ley, entrarán en vigencia una vez que dicho reglamento se encuentre dictado.

Artículo tercero.- El reglamento al que se refiere el artículo 30 de la presente ley deberá dictarse en un plazo de 12 meses contados desde la publicación de la presente ley en el Diario Oficial.

Artículo cuarto.- El mayor gasto fiscal que represente la aplicación de esta ley durante su primer año presupuestario de vigencia, será financiado con cargo a los recursos que se contemplen en el presupuesto del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, y en lo que faltare, el Ministerio de Hacienda podrá suplementarlo con cargo a los recursos de la partida del Tesoro Público, de la Ley de Presupuestos del Sector Público.”.

REPUBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

Dios guarde a V.E.,

GABRIEL BORIC FONT
Presidente de la República

CAROLINA TOHÁ MORALES
Ministra del Interior y
Seguridad Pública

ALBERT VAN KLAVEREN STORK
Ministro de Relaciones Exteriores

MAYA FERNÁNDEZ ALLENDE
Ministra de Defensa Nacional

MARIO MARCEL CULLELL
Ministro de Hacienda

ÁLVARO ELIZALDE SOTO
Ministro
Secretario General de la Presidencia

REPUBLICA DE CHILE
MINISTERIO
SECRETARIA GENERAL DE LA PRESIDENCIA

NICOLÁS GRAU VELOSO
Ministro de Economía,
Fomento y Turismo

JAVIERA TORO CÁCERES
Ministra de Desarrollo
Social y Familia

NICOLÁS CATALDO ASTORGA
Ministro de Educación

LUIS CORDERO VEGA
Ministro de Justicia
y Derechos Humanos

JUAN CARLOS MUÑOZ ABOGABIR
Ministro de Transportes
y Telecomunicaciones

AISÉN ETCHEVERRY ESCUDERO
Ministra de Ciencia, Tecnología,
Conocimiento e Innovación