LEY SOBRE INTELIGENCIA ARTIFICIAL

Proyecto de ley en discusión:

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, con enfoque de género, de las personas frente a los efectos nocivos que determinados usos pudieran irrogar.

A su vez, la presente ley tendrá por objeto la promoción de inteligencia artificial que fomente la igualdad de género.

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.

d) Sistemas de IA utilizados exclusivamente por usuarios finales.

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/o el distribuidor.

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

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

13. 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.

14. 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.

15. Incidente grave: todo incidente o defecto de funcionamiento de un sistema de IA que 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.

16. 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.

17. 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.

18. 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.

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

20. 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.

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

22. 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 operador en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

23. Sistema de IA de uso general: un sistema de IA capaz de realizar funciones de aplicación general y tener múltiples usos, tanto previsibles como no previsibles, como el reconocimiento de imágenes, reconocimiento de voz, procesamiento de audio, generación de video, detección de patrones, respuesta a preguntas, traducción, entre otros.

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 ilegal o arbitrario.

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 y/o utilización.

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.

i) Igualdad de género: se propenderá a que los sistemas de IA se desarrollen y utilicen como una herramienta para la promoción de igualdad de género y para la eliminación de cualquier discriminación basada en el género. Los datos utilizados para entrenar los sistemas deberán estar libres de sesgos de género, y los algoritmos deberán diseñarse de manera tal que eviten la reproducción de las desigualdades de género existentes.

j) Derechos de autor y derechos conexos: Los sistemas de IA se desarrollarán y utilizarán en estricto apego a la regulación de derecho de autor vigente y a los tratados internacionales suscritos y ratificados por Chile que regulan la materia.

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

El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, la Agencia de Protección de Datos Personales (en adelante, "APDP") y la Agencia Nacional de Ciberseguridad (en adelante, "ANCI"), incorporarán estos principios en las distintas orientaciones destinadas a prestar asistencia al operador en cuanto al modo de desarrollar y utilizar sistemas de IA, así como al momento de regular y fiscalizar 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 usos de 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) Uso de alto riesgo: Agrupa a sistemas de IA autónomos o componentes de seguridad de productos cuya utilización puede 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) Uso de riesgo limitado: Agrupa a sistemas de IA cuyo uso presentan riesgos no significativos de manipulación, engaño o error, producto de su interacción con personas naturales.

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

Título II

Uso de riesgo inaceptable de sistemas de inteligencia artificial

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

a) Manipulación subliminal: sistemas de IA que emplean técnicas imperceptibles para las personas y que tienen como objeto o efecto directo la inducción de acciones que causan daños a la salud física y/o mental.

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

Asimismo, se entenderán incluidos dentro de esta categoría aquellos usos de 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, aquellos cuyos usos pueda significar una vulneración de los derechos de niños, niñas y adolescentes, de acuerdo con lo dispuesto en la ley N°21.430.

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

Esta prohibición no se aplicará a los sistemas de IA destinados a ser utilizados para fines terapéuticos autorizados sobre la base de un consentimiento informado, específico y expreso, 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) Calificación social genérica: sistemas de IA que tienen por finalidad evaluar o clasificar a personas o grupos de personas naturales en función de su comportamiento social, su nivel socioeconómico o sus características personales o de personalidad conocidas o inferidas, de modo tal que su calificación resultante provoque una discriminación ilegal o arbitraria sobre dichas personas o grupos de personas.

e) Identificación biométrica remota en espacios de acceso público en tiempo real: sistemas de IA utilizados para el 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, ejecutar sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, de conformidad con la ley.

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

Título III

Uso de riesgo alto de sistemas de inteligencia artificial

Artículo 7.- Uso de Sistemas de IA de alto riesgo. La utilización de un sistema de IA se considerará de alto riesgo cuando presente un riesgo significativo de afectación de los derechos fundamentales protegidos por la Constitución Política de la República, ya sea que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto, o bien que sea en sí mismo dicho producto.

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

Artículo 8.- Reglas aplicables a los sistemas de IA de alto riesgo. Los sistemas de IA cuyos usos sean calificados 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 incidentes 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 de entrenamiento de modelos con datos deberán contar con una gobernanza de datos adecuada a su propósito y contexto de uso. Asimismo, deberán incorporar estándares de seguridad y protección de datos, incluyendo mecanismos de prevención y gestión de incidentes de seguridad de la información, según su ámbito de aplicación.

c) Documentación técnica: La documentación técnica requerida para el 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 deberán contar con funciones que permitan registrar información y eventos de seguridad mientras están en funcionamiento.

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

e) Mecanismos de transparencia y explicabilidad: Los sistemas de IA de alto riesgo deberán contar con un nivel de transparencia y explicabilidad suficiente para que los operadores y sus destinatarios entiendan razonablemente el funcionamiento del sistema, con arreglo a su finalidad prevista. Asimismo, deberán permitir que los usuarios identifiquen que están interactuando con un sistema de IA, salvo cuando esto sea evidente por las circunstancias y el contexto de uso.

En el uso de sistemas de IA de alto riesgo, se deberá emplear 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 deberán contar con mecanismos técnicos y operativos, que permitan su supervisión por personas naturales técnicamente capacitadas para esta función. La supervisión deberá garantizar que el sistema se utilice conforme a su finalidad prevista y, además, identificar y mitigar los riesgos asociados a un uso indebido razonablemente previsible, con el fin de evitar impactos negativos en los derechos fundamentales de las personas.

g) Precisión, solidez y ciberseguridad: El funcionamiento de los sistemas de IA de alto riesgo deberá respetar el principio de seguridad desde el diseño y por defecto, debiendo contar con un nivel adecuado de precisión, resiliencia, seguridad y ciberseguridad, funcionando de manera fiable, predecible y resiliente, garantizando su seguridad y resistencia a incidentes durante todo su ciclo de vida.

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

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.

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

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

Artículo 9.- Seguimiento posterior a la implementación, puesta en servicio, distribución e introducción en el mercado, de sistemas de IA de alto riesgo. Los operadores establecerán y documentarán un sistema de seguimiento, que sea proporcional y adecuado a la naturaleza y riesgos identificados en sus usos.

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

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

Título IV

Uso de riesgo limitado de sistemas de inteligencia artificial

Artículo 10.- 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.

Estos sistemas deberán garantizar condiciones de transparencia, explicabilidad y seguridad, proporcionales a su nivel de riesgo de modo tal que las personas sean informadas de forma clara y precisa, y les permitan reconocer que están interactuando con una máquina.

Artículo 11.- Obligaciones de transparencia y explicabilidad en el uso de sistemas de IA de riesgo limitado. Los operadores procurarán que los sistemas de IA de riesgo limitado informen de manera clara, inteligible y oportuna a las personas 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

Artículo 12.- Incidentes. Todo aquel que identifique un incidente, en los términos del numeral 15 del artículo 3 de la presente ley, podrá reportarlo a la Agencia de Protección de Datos Personales, la que, en el ámbito de sus competencias, informará de esta circunstancia al operador para que éste notifique a las personas afectadas.

Dicha notificación se efectuará tan pronto tome conocimiento del incidente, después de que el operador haya establecido un vínculo causal entre el uso del sistema de IA y el incidente, o la posibilidad razonable de que exista dicho vínculo. En cualquier caso, la notificación deberá realizarse a más tardar setenta y dos horas después de que el operador tenga conocimiento de dicho incidente.

Una vez que se haya establecido un vínculo causal entre el uso de un sistema de IA y el incidente, o la posibilidad razonable de que exista dicho vínculo, el operador adoptará inmediatamente las medidas necesarias ya sea para desactivarlo, retirarlo del mercado o suspenderlo, según corresponda.

Cuando el incidente involucre vulnerabilidades de ciberseguridad que afecten a servicios esenciales y operadores de importancia vital, según lo dispuesto en la ley N° 21.663, la APDP deberá notificar y coordinarse con la ANCI para su evaluación y respuesta.

Título VI

Gobernanza

Artículo 13.- Consejo Asesor Técnico de Inteligencia Artificial. Créase el Consejo Asesor Técnico de Inteligencia Artificial (el "Consejo Asesor de IA") como una instancia de carácter técnico, 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/a representante de la Secretaría de Gobierno Digital del Ministerio de Hacienda.

b) Un/a representante de la Agencia encargada de la Protección de Datos Personales.

c) Un/a representante de la Agencia Nacional de Ciberseguridad.

d) Un/a académico/a experto/a en derecho y tecnología.

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

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

g) Dos representantes de la industria de tecnología.

h) Dos representantes de organizaciones de la sociedad civil.

Los integrantes indicados en los literales a), b) y c) 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. Dichos nombramientos podrán ser modificados cuando la autoridad competente lo estime conveniente.

Por su parte, los integrantes mencionados en los literales d), e), f), g) y h) serán nombrados por la Ministra o el Ministro de Ciencia, Tecnología, Conocimiento e Innovación y durarán 2 años en sus cargos, con posibilidad de ser reelegidos consecutivamente por idéntico periodo. Las renovaciones a las que hace referencia este inciso se realizarán en un solo acto por la Ministra o el Ministro de Ciencia, Tecnología, Conocimiento e Innovación.

En la composición del consejo se deberá asegurar una representación con paridad de género.

El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación publicará una tabla con los temas que se tratarán en cada sesión del consejo. Los organismos públicos podrán manifestar su interés en participar, de acuerdo con su ámbito de competencia. Asimismo, la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación o la funcionaria o funcionario que designe al efecto podrá invitar a representantes de dichos organismos cuando los temas a tratar estén relacionados con sus competencias. También podrá invitar a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.

Artículo 14.- 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, cuyo uso, conforme a los criterios establecidos en la presente ley, y considerando especialmente aquellos que, por su naturaleza o impacto evidente, impliquen riesgos significativos 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 cuyo uso sea de alto riesgo y de riesgo limitado, así como las obligaciones y responsabilidades de los proveedores, implementadores, el

representante autorizado, el importador y/o el distribuidor definidos en el artículo 3 de esta ley.

Sin perjuicio de lo anterior, los sistemas de IA de uso general deberán dar siempre cumplimiento a las obligaciones establecidas en el artículo 8 de la presente ley.

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 15.- Informe anual del Consejo Asesor Técnico de Inteligencia Artificial. El Consejo Asesor Técnico de Inteligencia Artificial deberá elaborar a más tardar el 31 de diciembre de cada año, un informe que detalle el cumplimiento y avance de las tareas encomendadas al Consejo en virtud de la presente ley, además de un análisis de la normativa vigente. Adicionalmente, este informe deberá ser entregado a la Ministra o Ministro de Ciencia, Tecnología, Conocimiento e Innovación para su estudio y análisis.

El informe podrá contener recomendaciones de dictación, modificación o derogación de los preceptos legales o reglamentarios que estime necesarios para la correcta implementación y usos de los sistemas de inteligencia artificial en el país.

Este informe será remitido por intermedio del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación a la Comisión de Futuro, Ciencias, Tecnología, Conocimiento e Innovación de la Cámara de Diputadas y Diputados. Adicionalmente, el informe será publicado en el sitio web institucional del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación a fin de garantizar su acceso público.

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 seis 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 APDP. 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.

e) Coordinar con la ANCI en los casos en que la APDP, en el ejercicio de sus competencias, según lo dispuesto en la presente ley, detecte infracciones o vulnerabilidades derivadas del uso de sistemas de inteligencia artificial que puedan comprometer la seguridad de las redes, sistemas informáticos, servicios esenciales u operadores de importancia vital regulados en la ley N° 21.663. En tales situaciones, la

APDP remitirá los antecedentes a la ANCI para que, dentro de su ámbito de atribuciones, evalúe el riesgo y determine las medidas de seguridad pertinentes.

Asimismo, la APDP podrá solicitar a la ANCI un informe sobre la evaluación y tratamiento del incidente, sin perjuicio de las competencias propias de cada organismo. Dicho informe será considerado por la APDP al fundamentar sus decisiones y resoluciones.

f) Ejercer las demás funciones y atribuciones que la ley le encomiende.

Título VII

Medidas de apoyo a la innovación

Artículo 20.- Espacios controlados de pruebas para la IA. Los órganos de la administración del Estado con facultades fiscalizadoras y/o regulatorias, dentro de sus respectivas competencias, podrán habilitar espacios controlados de prueba que fomenten la innovación y permitan la investigación, desarrollo, prueba y la validación de sistemas innovadores de IA.

La habilitación de estos espacios deberá garantizar el respeto a los derechos fundamentales, la seguridad, la democracia y la protección del medioambiente, así como la prevención y mitigación de riesgos en ciberseguridad y protección de datos personales.

Los órganos que habiliten 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.

Un reglamento expedido por intermedio del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación establecerá los criterios mínimos para la creación, funcionamiento y supervisión de los espacios controlados de prueba. Los órganos que habiliten estos espacios deberán adecuar sus normativas internas conforme a este reglamento, estableciendo condiciones específicas de acceso, seguridad, evaluación de riesgos y mecanismos de supervisión aplicables a los sistemas que se prueben en dichos espacios.

En caso de que se detecte un riesgo significativo que pueda afectar los derechos fundamentales, la salud, la seguridad, la democracia, o el medio ambiente el operador del sistema de IA deberá adoptar medidas inmediatas y apropiadas de mitigación. De no implementarse adecuadamente estas medidas, los órganos competentes estarán facultados para suspender temporal o permanentemente la 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 operadores en los espacios controlados de pruebas para la IA responderán de cualquier perjuicio causado a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas.

Siempre y cuando los operadores respeten las disposiciones de esta ley, el reglamento a que se refiere el artículo precedente y las orientaciones proporcionada por los órganos de la Administración del Estado que habiliten estos espacios controlados de prueba, estarán exentos del pago de las multas administrativas a las que se refiere el artículo 24 de la presente ley, sin perjuicio de la responsabilidad por los daños que pudieren causar.

La utilización de un espacio controlado de prueba no es un requisito habilitante para el desarrollo, prueba y validación de los sistemas de lA, así como su distribución, introducción en el mercado, puesta en servicio, o cualquier actividad realizada por un operador, y no exime de las obligaciones y responsabilidades establecidas en esta ley.

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 en el uso de sistemas de IA. 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.

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

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

a) Gravísima: El uso de un sistema de IA que contravenga con lo dispuesto en el artículo 6 sobre usos de riesgo inaceptable. Se considerará además infracción gravísima la reincidencia de una misma infracción grave dentro de un año.

b) Grave: el incumplimiento de las reglas dispuestas en el artículo 8 para los usos de alto riesgo. Se considerará además infracción grave la reincidencia en una misma infracción leve dentro de un año.

c) Leve: el incumplimiento de las obligaciones de transparencia dispuestas respecto de los usos de sistemas de IA de riesgo limitado del artículo 10. Se considerará además infracción leve cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

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

Artículo 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 uso y alcance del sistema de IA, así como, cuando proceda, la gravedad, intensidad, probabilidad de ocurrencia y duración de sus efectos, así como el número de personas afectadas y el nivel de los daños ocasionados.

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.

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

5. El rol específico que cumple el proveedor, implementador, representante autorizado, importador y/o distribuidor en la cadena de valor de la inteligencia artificial.

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

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

a) El procedimiento sancionatorio será instruido por la Agencia de Protección de Datos Personales, de acuerdo con sus competencias y atribuciones legales.

b) La Agencia de Protección de Datos Personales podrá iniciar un procedimiento sancionatorio, de oficio o petición de parte. Al inicio del procedimiento, la APDP deberá dictar una resolución que disponga la apertura del expediente y designar un funcionario o funcionaria responsable de la instrucción del procedimiento.

c) La APDP deberá presentar una formulación de cargos que deberá contener una descripción clara y precisa de los hechos que configuran la infracción 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 conforme a lo dispuesto en los artículos 46 y 47 de la ley N°19.880, 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 posteriores.

f) Si existen hechos sustanciales, pertinentes y controvertidos, la APDP podrá disponer la apertura de un periodo probatorio de hasta diez días hábiles. Este plazo se contará desde el día siguiente a la notificación de la resolución que ordene su inicio, conforme a lo establecido en el artículo 25 de la ley N°19.880. Durante este período, podrán presentarse todos los medios de prueba admisible en derecho.

g) La Agencia de Protección de Datos Personales 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 decisión.

h) Los hechos investigados y determinación de las responsabilidades se regirán por las reglas de valoración de la prueba conforme a la sana crítica.

i) La Agencia de Protección de Datos Personales tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a la determinación de la infracción y sus efectos.

j) La resolución que dicte la APDP deberá ser fundada y resolver todas las cuestiones planteadas en los cargos, 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, la sanción correspondiente o la absolución de cargo. Esta resolución deberá ser notificada al operador e 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.

k) En caso de que la Agencia de Protección de Datos Personales 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 con la gravedad de la infracción cometida, conforme a los criterios establecidos en esta ley.

l) El procedimiento administrativo de infracción de ley no podrá superar los seis meses, salvo que circunstancias excepcionales, debidamente fundamentadas, justifiquen su prórroga por una única vez.

Artículo 27.- Procedimiento de reclamación judicial. Las reclamaciones judiciales derivadas del ejercicio de los derechos y obligaciones establecidos en la presente ley se regirán por el procedimiento contemplado en el artículo 43 de la ley N° 19.628.

Los tribunales competentes conocerán de estas reclamaciones conforme a lo dispuesto en la referida normativa en el marco del uso de sistemas de inteligencia artificial.

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

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, cuando exista peligro inminente de daño irreparable.

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 10, respectivamente.

El reglamento especificará, adicionalmente, lo siguiente:

a) El contenido mínimo y forma dar cumplimiento a las reglas aplicables a los sistemas de IA, cuyo uso sea calificado de alto riego según lo dispuesto en el artículo 8.

b) 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.

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

d) Las obligaciones y responsabilidades que deberán cumplir los operadores de sistemas de IA cuyo uso sea de alto riesgo y de riesgo limitado, conforme a lo señalado en el artículo 3 de esta ley y en función de las reglas establecidas para cada tipo de sistema de IA.

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 y extracción de obras publicadas de forma legítima para fines de minería de textos y datos, siempre que esta utilización se efectúe sin fines lucrativos y para fines de investigación.

Los titulares podrán optar, en relación al inciso anterior, por reservarse sus derechos.

DISPOSICIONES TRANSITORIAS

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

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.

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.

Lo dispuesto en el artículo 25 entrará en vigencia a los 6 meses de la entrada en vigencia del reglamento mencionado en el inciso primero.

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.".