

Rad. 2024201829
Cod. 9000
Bogotá, D.C.

Radicado:	2024532391
Fecha:	17/10/2024 4:27:14 P. M.
Proceso:	9000 INNOVACIÓN Y PROSPECTIVA REGULATORIA
Destino:	CÁMARA DE REPRESENTANTES
Asunto:	COMENTARIOS AL PROYECTO DE LEY NRO. 154 DE 2024 CÁMARA. PONENCIA PARA PRIMER DEBATE.

Señora Secretaria
AMPARO YANETH CALDERÓN PERDOMO
Secretaria
COMISIÓN PRIMERA CONSTITUCIONAL
CÁMARA DE REPRESENTANTES
comisión.primer@camara.gov.co; debatescomisionprimera@camara.gov.co

Asunto: Comentarios al Proyecto de Ley nro. 154 de 2024 Cámara. Ponencia para primer debate.

Estimada doctora Amparo:

Un saludo cordial de parte de la Comisión de Regulación de Comunicaciones (CRC). Hemos tenido conocimiento de la ponencia para primer debate de la propuesta del Proyecto de ley «*Por la cual se define y regula la inteligencia artificial, se ajusta a estándares de derechos humanos, se establecen límites frente a su desarrollo, uso e implementación se modifica parcialmente la Ley 1581 de 2012 y se dictan otras disposiciones*», (en adelante, Proyecto de ley).

En atención a esta solicitud, esta entidad como parte del Sector administrativo de Tecnologías de la Información y las Comunicaciones, según lo dispuesto en el artículo 19 de la Ley 1341 de 2009, modificado por la Ley 1978 de 2019, presenta las siguientes observaciones al articulado, orientadas a contribuir al desarrollo ético y responsable de la Inteligencia Artificial en el país.

1. Comentarios generales al Proyecto de ley

En la última década la Inteligencia Artificial (IA) ha alcanzado su mayor impulso. Dicho crecimiento se ha dado gracias a la integración de la IA con otras tecnologías como la computación en la nube, el *big data* y el aprendizaje automático (*Machine Learning*). Es así como hoy la IA se emplea en diferentes campos como la medicina, la agricultura, las finanzas y la educación, entre otros, logrando transformar y mejorar las actividades y procesos en estos diferentes campos.

En países como Estados Unidos, China, Reino Unido y Alemania la tecnología de IA ha tenido un importante desarrollo. Lo que ha generado que varios países y organizaciones internacionales hayan expedido políticas y normas relacionadas con la IA, con foco en las oportunidades y transformación que genera el desarrollo de esta tecnología y con especial atención en la implementación responsable de sistemas de IA.

Lo anterior se puede observar en la versión 2024 del *AI Index Report del HAI (Human-Centered Artificial Intelligence)*¹ de la Universidad de Stanford, en la cual se indica que: «Las menciones a la

¹ El reporte puede ser consultado en <https://aiindex.stanford.edu/report/#individual-chapters>

IA en los procedimientos legislativos de todo el mundo casi se han duplicado, pasando de 1.247 en 2022 a 2.175 en 2023. La IA se mencionó en los procedimientos legislativos de 49 países en 2023. Además, al menos un país de cada continente habló de la IA en 2023, lo que subraya el alcance verdaderamente global del discurso sobre políticas de IA»².

El aumento en la normatividad internacional relacionada con la IA refleja la necesidad que tienen los diferentes gobiernos de evaluar el impacto de los sistemas de IA y mitigar los riesgos que podría generar su uso. Pero también evidencia, que cada vez los países buscan mejorar la capacidad de investigación, la formación de talento humano, la inversión y la infraestructura tecnológica, entre otros, para que cada país pueda aprovechar el potencial transformador de la IA.

Es así como los países han adoptado diferentes enfoques al expedir regulación de la IA. Países como Estados Unidos o Reino Unido, tienen un modelo de autorregulación dirigido a incentivar el desarrollo, la implementación y el uso responsable de la IA. Por su parte, la Unión Europea establece un marco legal y ético para el desarrollo y uso de la IA, definiendo acciones concretas para garantizar que los sistemas de IA sean seguros, respeten los derechos fundamentales, aseguren la privacidad de los datos personales y eviten los sesgos y la discriminación. De otro lado, China ha adoptado un enfoque de control estricto para el desarrollo y uso de la IA, supervisando de cerca el avance de la IA para asegurar que se alinee con los objetivos y valores de ese gobierno.

En el caso de Colombia de tiempo atrás se han venido generando disposiciones asociadas a las siguientes temáticas:

- En noviembre de 2021 Colombia se unió a las Recomendaciones de la UNESCO sobre la ética en la IA.
- El Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic) lanzó en septiembre de 2023 la estrategia «Colombia PotenciA Digital», la cual tiene como objetivo acelerar los ecosistemas de innovación y transformación digital en todas las regiones del país. La estrategia se basa en tres ejes: conectividad, educación y ecosistemas.
- El Ministerio de Ciencia, Tecnología e Innovación (Minciencias) lanzó en febrero de 2024 «La Hoja de Ruta de la Inteligencia Artificial (IA)» que tiene como objetivo garantizar la adopción ética y sostenible de la IA.
- El 22 de mayo de 2024, el Mintic radicó el Proyecto de ley «Por medio de la cual se dictan disposiciones para el suministro, intercambio y aprovechamiento de la infraestructura de datos del Estado colombiano (IDEC) y la interoperabilidad de los sistemas de información de las entidades públicas», que busca desarrollar una infraestructura de datos sólida, segura y de calidad; aumentar la disponibilidad, uso e intercambio de datos; mejorar la toma de decisiones y consolidar una cultura de datos en el país; para convertir a Colombia en PotenciA Digital.
- El Departamento de Planeación Nacional (DNP) trabaja en la expedición del CONPES de IA, que tiene como objetivo impulsar las oportunidades de aprovechamiento y democratización de la IA, teniendo como referentes los principios éticos y la protección de

² El Índice de IA realizó la búsqueda de la palabra clave «inteligencia artificial» en los sitios web de los congresos o parlamentos de 128 países

los derechos humanos.

- El 20 de septiembre de 2024, se suscribió un memorando de entendimiento, entre la Comisión Accidental de la Comisión Sexta del Senado de la República de Colombia³, el Ministerio de Tecnologías de la Información y las Comunicaciones; el Ministerio de Ciencia, Tecnología e Innovación; y, los expertos y la ciudadanía interesada, con el objetivo de proveer acompañamiento técnico en el análisis de regulaciones y políticas en materia de Inteligencia Artificial.

Además, en el legislativo cursan varios proyectos de Ley que tienen diferentes finalidades, tales como: establecer de manera general los lineamientos de política pública para el desarrollo uso e implementación de la IA; definir condiciones para la entrega de información e intercambio de datos; armonizar la IA con el derecho al trabajo; definir lineamientos de uso de la IA en la disminución de siniestros viales; o el Proyecto de ley 154-2024C, objeto de comentarios en la presente comunicación, que busca regular el desarrollo de la IA y establecer límites frente a su uso e implementación.

Previo a definir obligaciones legislativas o regulatorias estrictas, es importante conocer el estado de uso y desarrollo de la IA en Colombia, identificar las numerosas oportunidades que crea para las empresas, la investigación, el Gobierno y la vida privada el desarrollo de la IA, así como también los posibles riesgos actuales y futuros. Dado que solo así, se podrán identificar cuáles son las acciones que se deben impulsar para el adecuado desarrollo de la IA en el país, cuáles son los riesgos que deben ser controlados y las acciones que se podrían adelantar para mitigar dichos riesgos.

Una fuente actualizada para conocer el estado de avance de la IA en América Latina y el Caribe es el Índice Latinoamericano de Inteligencia Artificial (ILIA)⁴. El índice, que publicó su segunda versión en septiembre del presente año, es elaborado por el Centro Nacional de Inteligencia Artificial de Chile (CENIA) y la Comisión Económica para América Latina y el Caribe (CEPAL), y enfoca su análisis en tres dimensiones: i) Factores Habilitantes; ii) Investigación, Desarrollo y Adopción; y iii) Gobernanza.

El índice permite conocer los puntajes relativos en cada una de las tres dimensiones, e identificar las fortalezas y debilidades de cada país en las variables definidas para cada dimensión. Además, establece una clasificación de acuerdo con el estado de desarrollo de cada país. Esta clasificación incluye tres niveles: «Explorador», «Adoptante» y «Pionero».

El índice sitúa a Colombia en el nivel «Adoptante» junto con países, como: Argentina, México, Republica Dominicana, Perú, Costa Rica, Panamá y Ecuador. De acuerdo con la definición del índice, los países en este nivel corresponden a aquellos que:

- Han comenzado a integrar la IA en diversos sectores de su economía y sociedad, pero que

³ Encargada de analizar y proponer regulaciones y políticas en materia de inteligencia artificial.

⁴ La segunda versión del Índice Latinoamericano de Inteligencia Artificial (ILIA) puede consultarse en el enlace <https://indicelatam.cl/>

- aún no alcanzan una posición de liderazgo.
- Están utilizando la IA en los sectores productivos, servicios y administraciones públicas, pero de manera incipiente.
- En el ámbito de la investigación, han logrado avances significativos en IA, aunque todavía no a la escala de los países pioneros.
- Están desarrollando estrategias y mostrando disposición para invertir y colaborar con otros estados para fortalecer sus capacidades en esta tecnología emergente.

Dicho lo anterior, y toda vez que la gestión de riesgos de la IA es un componente clave del desarrollo y uso responsable de los sistemas de IA, la CRC observa que el Proyecto de Ley de la referencia, no tiene en cuenta que la IA, al igual que cualquier otra tecnología, está en constante evolución y que la definición de prohibiciones explícitas en normas de jerarquía de ley (incluso estatutaria), sin un análisis del contexto, pueden impedir el desarrollo y la adopción de esta tecnología en el país y, por lo tanto, alejarnos del cumplimiento de los objetivos expuestos por el HR Alirio Uribe Muñoz, quien indicó en la Audiencia Pública del Proyecto de ley que "la IA llegó para quedarse [...] y la normatividad no puede limitar las innovaciones tecnológicas, dado que la IA es un instrumento que nos puede ayudar a vivir mejor, dependiendo de las políticas que se adopten".

Así mismo, el Proyecto de ley en comento pierde de vista que todo sistema de IA tiene un ciclo de vida conformado por el diseño, el entrenamiento, la implementación y el uso, y que una o varias etapas del ciclo de vida pueden conformar el modelo⁵ o el sistema⁶ de IA y ser desarrolladas a nivel nacional o internacional. Por lo cual, muchas de las obligaciones que están siendo definidas en el articulado del Proyecto de ley, tales como la clasificación de riesgo, la publicación de la evaluación de los riesgos, las auditorías a los algoritmos, no tienen unas condiciones claras para su implementación, lo cual propiciaría una confusión en el cumplimiento con posibles efectos adversos para el adecuado desarrollo y uso de sistemas de IA en el país, lo cual podría repercutir negativamente entre otros aspectos : (i) obstaculizar el desarrollo de la innovación, al reducir el interés de adelantar actividades de investigación y desarrollo; (ii) generar costos adicionales, que afecten especialmente a las pequeñas empresas; (iii) impulsar la desigualdad en el acceso y desarrollo de los diferentes países; o (iv) generar obstáculos técnicos al comercio.

Así las cosas, con el objetivo de obtener el potencial transformador de la IA para el país y disminuir los riesgos para el uso responsable de la IA, el enfoque de la normatividad general deberá basarse en la **definición de principios** que aborden, temas como: (i) la protección de la privacidad, para evitar el uso indebido de datos personales; (ii) la seguridad, de tal forma que el uso de sistemas de IA no represente un peligro para el usuario; (iii) la equidad e inclusión, para que los algoritmos minimicen sesgos y potencial discriminación; y (iv) la transparencia, que permita conocer cómo funcionan los algoritmos y cómo se toman las decisiones.

Igualmente, para que los marcos regulatorios sigan el ritmo del desarrollo de la IA; preserven los derechos de todos los sectores; brinden flexibilidad para su desarrollo en pequeñas y grandes

⁵ Representación matemática de un proceso que se ha entrenado con datos.

⁶ Conjunto de varios componentes, incluidos uno o varios modelos.

empresas; ayuden a fomentar el diseño, desarrollo, la implementación y el uso responsable de la IA; es necesario que el desarrollo de las condiciones para el cumplimiento de dichos principios quede a cargo de una autoridad administrativa que determine la ley, para de esta forma garantizar que las normas expedidas sean adecuadas al propósito definido.

Por las razones expuestas, solicitamos respetuosamente el archivo del Proyecto de ley 154 de 2024C, y dado que debe ser una prioridad para el Estado como un todo, impulsar el desarrollo de los sistemas de IA y minimizar los posibles impactos negativos, desde la CRC consideramos que todos los esfuerzos pueden ser consolidados a través de la Comisión Accidental Bicameral, encargada de establecer un marco normativo sólido y claro que garantice que la Inteligencia Artificial se desarrolle de manera ética, responsable y en beneficio de toda la sociedad.

2. Comentarios específicos al articulado del Proyecto de ley

No obstante considerar, que el análisis de la gobernanza de IA debe darse bajo un único seno de debate para lograr consensos y escuchar la totalidad de las opiniones en un mismo foro, con el ánimo de contribuir con el proceso de conversación y creación de las iniciativas legislativas, a continuación, se formulan algunos comentarios sobre el articulado del Proyecto de Ley de la referencia:

- **ARTÍCULO 1. OBJETO.** La presente ley tiene por objeto definir y regular la inteligencia artificial ajustándola a estándares de respeto y garantía de los derechos humanos, así como para regular y promover su desarrollo y establecer límites frente a su uso, implementación y evaluación por parte de personas naturales y jurídicas.

Comentario:

El objeto propuesto establece de manera general la regulación de la Inteligencia Artificial (IA), desconociendo que la IA está conformada por algoritmos, modelos, datos, sistemas, *hardware* y *software*. Dicha definición podría dar a entender que el Proyecto de ley busca regular desde la creación misma de un modelo matemático, el cual nunca sea usado en un sistema de IA.

Algo semejante ocurre con la última parte del objeto propuesto, el cual indica que se van a «establecer límites frente a su uso [de la inteligencia artificial], implementación y evaluación por parte de personas naturales y jurídicas», sin que se determine si dichos límites van a estar enfocados a prevenir riesgos generados por el uso e implementación de sistemas de IA o cuál es la condición para definir dichas limitaciones. Con lo cual se podría llegar a discernir que la limitación al uso, implementación y evaluación de los sistemas de IA se realizaría de manera general sin que exista un uso concreto que genere un riesgo.

Para poder determinar el objeto del Proyecto de ley es importante revisar la definición realizada por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la cual indica que la IA es «un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir

de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden incluir en entornos físicos o virtuales».

Así las cosas, sugerimos la siguiente modificación en la redacción del objeto: «La presente ley tiene por objeto establecer las condiciones aplicables a los sistemas de Inteligencia Artificial, para promover su desarrollo y el respeto de los derechos humanos». Para acoger lo dispuesto por la OCDE.

- **ARTÍCULO 2. ÁMBITO DE APLICACIÓN.** Las disposiciones de esta ley son aplicables al diseño, innovación, aplicación, uso y desarrollo de la inteligencia artificial por parte de personas naturales o jurídicas, así como a los proveedores, productores o demás agentes que participen en el desarrollo de la inteligencia artificial nacionales y extranjeros, salvo en los casos donde resulte aplicable una regulación especial.

Los principios y disposiciones contenidos en la presente ley serán aplicables a:

- a. Los Productores que desarrollen inteligencia artificial y/u ofrezcan o comercialicen la inteligencia artificial en territorio colombiano o fuera del territorio colombiano, si el funcionamiento de la inteligencia artificial produce efectos en el territorio colombiano.
- b. Los proveedores que ofrezcan y presten el servicio de instalación y funcionamiento inteligencia artificial fuera del territorio colombiano, si la instalación y funcionamiento de inteligencia artificial produce efectos en el territorio colombiano.
- c. Los usuarios de la inteligencia artificial ubicados en el territorio colombiano.

La regulación contenida en esta Ley Estatutaria no aplicará a la inteligencia artificial que:

- a. Se desarrolla en el marco de actividades de carácter educativo o académico o científico en instituciones educativas de educación básica primaria y básica secundaria e instituciones de educación superior ubicadas en el territorio colombiano, siempre que la inteligencia artificial no se instale y entre en funcionamiento de manera permanente en la misma institución, actividades de terceros o por fuera del ámbito educativo o científico.

En todo caso, cualquier institución educativa que pretenda desarrollar proyectos temporales de inteligencia artificial deberá conformar un comité de ética que conocerá de estos proyectos, exigirá planes de manejo del riesgo ético y los hará cumplir dentro de los lineamientos establecidos en la Ley 10 de 1990, o aquella que haga sus veces, y en las normas de origen legal y administrativo

- b. Sea empleada por usuarios persona natural no comerciante en el marco de actividades de índole personal y no profesionales o que afecten a terceros.

Comentario:

Para definir los sujetos identificados en el ámbito de aplicación a los cuales le serían aplicables las obligaciones establecidas en el Proyecto de ley es necesario primero que todo identificar cuál es el ciclo de vida de la IA, dado que en cada una de las etapas de dicho ciclo interactúan diferentes agentes, los cuales pueden ser nacionales o extranjeros.

Una vez definidos dichos agentes, es necesario poder identificar cómo le serían aplicables las condiciones establecidas en la normatividad nacional y si dichas condiciones pueden llegar a establecer alguna restricción al libre comercio.

Cabe destacar que la OCDE definió las siguientes 4 etapas que conforman el ciclo de vida de la IA:

- **Diseño, datos, y modelado:** conformada por la planificación y diseño del sistema de IA, la recopilación y procesamiento de datos que se utilizarán para el entrenamiento de los modelos, la creación o selección de modelos y arquitectura, y el entrenamiento e interpretación de una tarea.
- **Verificación y validación:** implica ejecutar y ajustar modelos, evaluando el rendimiento en diversas dimensiones.
- **Implementación:** corresponde a las pruebas piloto para verificar la compatibilidad de sistemas, gestionar el cambio organizacional y evaluar la experiencia de usuario.
- **Funcionamiento y monitoreo:** se basa en el funcionamiento de los sistemas de IA para evaluar el rendimiento del modelo, sus recomendaciones e impactos, con el fin de identificar problemas, mejorar rendimientos y realizar ajustes en alguna de las fases mediante la optimización de los parámetros del modelo.

Ahora bien, para el desarrollo de estas etapas se requieren datos, chips aceleradores de IA, infraestructura informática y capacidad en la nube, pero el artículo propuesto no es claro en el sentido de indicar si, cuando se hace referencia a los productores de IA, se incluyen todos los actores que participan en las diferentes etapas, lo cual puede generar vacíos y problemas en la implementación de la Ley.

Por su parte, el desarrollo de modelos de IA presenta distintos grados de apertura, tales como:

- (i) modelos completamente abiertos (donde se proporciona acceso al código fuente y a los pesos y datos de entrenamiento);
- (ii) modelos parcialmente abiertos (donde se proporciona acceso a los pesos entrenados por el modelo, pero no al código fuente);
- (iii) modelos de código cerrado (accesibles a través de API, es decir, se da acceso a la salida, pero no al código fuente); y
- (iv) completamente cerrados (donde no se proporciona acceso al código fuente, los pesos o la salida).

Dejando a salvo, las dificultades evidentes que podrían presentarse al momento de hacer efectiva la regulación respecto de agentes que se encuentren por fuera del territorio colombiano, se observa que en el ámbito de aplicación de la disposición analizada se establece, como eje central de los supuestos a) y b), si el funcionamiento de la inteligencia artificial *produce efectos en el territorio colombiano*. Esta consagración debido a su amplitud y abstracción no permite determinar el alcance concreto del impacto, puesto que en principio la redacción propuesta recogería cualquier tipo de consecuencia o resultado del uso de la IA.

Ahora bien, en particular, el literal b) propuesto hace referencia a los proveedores que instalen o pongan en funcionamiento IA fuera de Colombia pero que produzca efectos dentro del territorio nacional, desconociendo así que los modelos de IA parcial o totalmente abiertos son una herramienta valiosa para la comunidad de desarrolladores o usuarios, gracias a que fomentan la innovación para aprovechar al máximo las capacidades de la IA de manera colaborativa.

Un ejemplo de estos modelos abiertos es *Hugging Face Transformers* que proporciona una biblioteca abierta de modelos de Procesamiento de Lenguaje Natural (NLP) como GPT-3⁷, T5⁸ y BERT⁹, para que los desarrolladores y usuarios desarrollen aplicaciones tales como chatbots, asistentes virtuales o análisis de texto. Así las cosas, en caso de un modelo abierto este puede ser modificado por diferentes personas y la responsabilidad ya no estaría a cargo del desarrollador del modelo, sino de quien lo modificó y lo utilizó en un sistema de IA.

Por otra parte, frente a la identificación de los sujetos a los que no es aplicable la regulación, no es claro si la exclusión establecida, en el artículo propuesto, solo aplica a los sistemas de IA desarrollados en el marco de actividades de carácter educativo o académico o científico, o también aplica a los sistemas de IA que no son desarrollados, sino que son utilizados en el marco de dichas actividades.

Además, es importante precisar que los proyectos de investigación y desarrollo no necesariamente se adelantan en instituciones educativas. Por lo cual, recomendamos incluir al sector privado que también puede adelantar actividades de investigación y desarrollo de sistemas o modelos de IA, antes de su puesta en servicio a nivel comercial.

- **ARTÍCULO 3. DEFINICIONES. Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Comentario:

De manera atenta solicitamos respetuosamente suprimir la definición de «Dato personal» dado que ya se encuentra desarrollada en la Ley 1581 de 2012 «Por la cual se dictan disposiciones generales para la protección de datos personales».

- **ARTÍCULO 3. DEFINICIONES. Productor de inteligencia artificial:** Persona natural o jurídica nacional o extranjera, pública o privada, que diseña, produce, implementa y desarrolla la inteligencia artificial en el mercado o para actividades concretas de un usuario.

⁷ GPT-3 modelo basado en el aprendizaje profundo, que permite generar textos de forma automática

⁸ T5 modelo de lenguaje desarrollado por Google AI que ha revolucionado la forma en la que las máquinas comprenden y generan texto.

⁹ BERT es el último algoritmo de búsqueda de Google.

Comentario:

Dado que el modelo de IA es utilizado para realizar predicciones o tomar decisiones, las cuales están basadas en el proceso de entrenamiento de los algoritmos, y que un sistema de IA puede incluir varios modelos que trabajan juntos para realizar una tarea. Se recomienda ajustar la definición, así: «Persona natural o jurídica nacional o extranjera, pública o privada, que diseña, produce, desarrolla e implementa modelos o sistemas de inteligencia artificial para su comercialización, o para actividades concretas de un usuario que no estén a disposición del público en general».

- **ARTÍCULO 3. DEFINICIONES. Proveedor de inteligencia artificial:** Persona natural o jurídica nacional o extranjera, pública o privada, que ofrezca, suministre, distribuya, comercialice o instale la inteligencia artificial en el mercado o para actividades concretas de un usuario.

Comentario:

En la misma línea de los comentarios a la definición anterior, se recomienda ajustar la definición propuesta, así: «Persona natural o jurídica nacional o extranjera, pública o privada, que ofrezca, suministre, distribuya, comercialice o instale sistemas de inteligencia artificial usados en actividades comerciales o empresariales o en actividades concretas de un usuario».

Ahora bien, en relación con las demás definiciones incluidas en el Proyecto de ley, se recomienda hacer referencia al estándar ISO/IEC 22989 publicado en 2022, el cual establece una base común de conceptos y terminología en el campo de la IA.

Adicionalmente, también se recomienda hacer seguimiento al resultado del Quinto Simposio Global sobre Normas (GSS-24) organizado por la UIT, el cual se realizará del 14 al 24 de octubre de 2024 en Nueva Delhi (India).

- **ARTÍCULO 4. PRINCIPIOS.** El desarrollo, interpretación y aplicación de la presente ley se realizará con arreglo a los siguientes principios:

[...]

Comentario:

En noviembre de 2021, Colombia se adhirió a las Recomendaciones de la UNESCO sobre la ética en la IA, las cuales integran valores y principios en políticas públicas para fortalecer evaluaciones de impacto, mecanismos de gobernanza, políticas éticas de datos, y promover un entorno propicio para la ética de la IA. No obstante, se evidencia que el artículo propuesto en el Proyecto de ley, si bien incluye algunos de los principios recomendados por la UNESCO, está adicionando otros principios y modificando la descripción de los ya existentes.

Es importante destacar que, la Recomendación de la UNESCO fue discutida con expertos de 155 países, la sociedad civil (mediante una encuesta mundial en línea), organismos de las

Naciones Unidas, grandes empresas mundiales, como Google, Facebook y Microsoft, así como el sector académico, con lo cual se podría llegar a entender que ya hay un proceso de discusión frente a los principios identificados y su definición, por lo que está Comisión no considera necesaria la inclusión de otros principios en el Proyecto de ley.

Sin embargo, si lo que se busca es incluir principios que estén adaptados a las necesidades del país, esta comisión recomienda revisar el «Marco ético para la Inteligencia Artificial en Colombia» en el cual se identificaron nueve principios éticos, resultado de 6 mesas técnicas lideradas por diferentes entidades de orden nacional e internacional, entre las cuales se encuentran la CAF, el BID y la universidad de Harvard a través del Berkman Klein Center for Internet & Society.

- **ARTÍCULO 4. PRINCIPIOS.** El desarrollo, interpretación y aplicación de la presente ley se realizará con arreglo a los siguientes principios:

[...]

Principio de Responsabilidad: Las personas que se vean perjudicadas con ocasión de los impactos negativos o vulneración generada del desarrollo de la inteligencia artificial, tendrán garantizado el derecho a reclamar indemnización o reparación a la que haya lugar ante las entidades públicas o privadas responsables.

Comentario:

El principio de responsabilidad está redactado como la consecuencia que se derivaría de una acción o evento por no aplicar un principio, y no como la regla que debe guiar el funcionamiento del sistema.

En consecuencia, se recomienda la siguiente redacción para el principio de responsabilidad, la cual además es congruente con la definición realizada por la UNESCO, «La responsabilidad ética y la obligación de rendir cuentas de las decisiones y las acciones basadas de alguna manera en un sistema de IA siempre deberían ser atribuibles, a los actores de la IA conforme a la función que tengan en el ciclo de vida del sistema de IA»

- **ARTÍCULO 4. PRINCIPIOS.** El desarrollo, interpretación y aplicación de la presente ley se realizará con arreglo a los siguientes principios:

[...]

Principio de Supervisión y Prevalencia de la Inteligencia Humana: Se preferirá la decisión humana respecto de los resultados derivados de la Inteligencia Artificial. Toda decisión tomada con base en los resultados de sistemas de inteligencia artificial será susceptible de revisión humana. La responsabilidad ética y legal de estas decisiones recaerá sobre las personas naturales o jurídicas involucradas en su uso.

Comentario:

La supervisión humana en IA busca asegurar que las decisiones tomadas por los sistemas de IA funcionen de manera ética, segura y efectiva. Por lo tanto, los sistemas de IA deben estar diseñados para ser supervisados eficazmente por personas físicas, con el objetivo de prevenir o minimizar los riesgos, detectar y corregir errores o comportamientos inesperados.

Dado lo anterior, se recomienda la siguiente redacción para el principio de supervisión: «Se garantizará la supervisión humana durante el entrenamiento de los modelos de IA y el uso de los sistemas de IA implementados, permitiendo que el humano tenga la capacidad de anular o revertir la salida del sistema de IA. En todo caso, un sistema de IA nunca podrá reemplazar la responsabilidad final de los seres humanos y su obligación de rendir cuentas».

- **ARTÍCULO 4. PRINCIPIOS.** El desarrollo, interpretación y aplicación de la presente ley se realizará con arreglo a los siguientes principios:

[...]

Principio de Seguridad y Protección: La información que permita desarrollar algoritmos y crear programas informáticos deberá gozar de confidencialidad e integridad.

Comentario:

Para el principio de seguridad y protección, se recomienda la siguiente redacción: «Los datos usados para el entrenamiento de los algoritmos y la creación o implementación de modelos de IA, deberán contar con soluciones que prevengan el ataque malintencionado a dichos datos de entrenamiento, así como también gozar de confidencialidad e integridad».

- **ARTÍCULO 6. CLASIFICACIÓN DEL RIESGO DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL.** Los sistemas o programas informáticos que usen e implementen la inteligencia artificial serán identificados según el riesgo por los productores y proveedores de la siguiente manera:

Riesgo inaceptable: Constituye riesgo inaceptable aquel que genera afectación a la seguridad, la subsistencia y los derechos humanos y fundamentales, y por tanto está proscrito.

Alto riesgo: Constituye alto riesgo aquel que, no siendo inaceptable, corresponde a actividades susceptibles de automatización admisibles bajo el mantenimiento de la calidad de los datos y facilidad de supervisión humana pero que eventualmente puede limitar algunos derechos humanos y fundamentales.

Riesgo limitado: Constituye riesgo limitado aquel que se deriva del uso e implementación de chatbots o robots conversacionales.

Riesgo nulo: Constituye riesgo nulo aquel derivado del uso e implementación de sistemas que no afectan los derechos y la seguridad de los usuarios.

PARÁGRAFO 1. La clasificación de riesgos genera obligaciones diferenciadas para los proveedores y usuarios, según lo contemplado en la ley.

PARÁGRAFO 2. Dentro del Reglamento que se expida se deberán identificar los sistemas o programas de inteligencia artificial que se consideren de riesgo inaceptable, alto riesgo, riesgo limitado y riesgo nulo. El reglamento deberá contar con actualización periódica de los sistemas o programas teniendo en cuenta los avances de este tipo de tecnologías y también el tipo de industria o sector que provea o use estos sistemas.

Comentario:

El citado artículo establece la definición del nivel de riesgo que generan los sistemas o programas informáticos que usen e implementen la inteligencia artificial, con lo cual se regula de manera específica los usos concretos de los sistemas de IA.

No obstante, como lo indica el documento [«Marco de Gestión de Riesgos de la IA» del Instituto Nacional de Estándares y Tecnología \(NIST\)](#) «Los riesgos pueden surgir de diversas formas y pueden caracterizarse como de largo o corto plazo, de alta o baja probabilidad, sistémicos o localizados y de alto o bajo impacto».

Así las cosas, definir el nivel de riesgo para un sistema IA es algo estático, mientras que la gestión eficaz del riesgo daría lugar a sistemas de IA más fiables, lo que generaría posibles beneficios para las personas y las empresas. La gestión de riesgos puede permitir a los desarrolladores y usuarios de IA comprender los impactos y tener en cuenta las limitaciones e incertidumbres inherentes a sus modelos y sistemas, lo que a su vez puede mejorar el rendimiento general del sistema.

Por su parte, el estándar ISO/IEC 23894, publicada en febrero de 2023, proporciona directrices específicas para la gestión de riesgos asociados con la IA. Esta norma fomenta la instalación de prácticas seguras y responsables en la implementación y uso de sistemas de IA. El enfoque principal del estándar es identificar, evaluar y mitigar los riesgos potenciales que la IA puede conllevar, tales como fallos técnicos, errores algorítmicos, y vulnerabilidades en la seguridad de datos.

La norma permite a las organizaciones desarrollar estrategias de gestión de riesgos que les permitan reaccionar rápidamente ante cualquier problema emergente, minimizando así el impacto negativo en sus operaciones y en la confiabilidad de sus sistemas. Además, promueve una cultura de prevención, ayudando a las organizaciones a mantenerse por delante de los posibles desafíos mediante la adopción de medidas proactivas.

Dado lo anterior, el Proyecto de ley no debería ser el mecanismo para regular de manera exhaustiva la clasificación de los riesgos asociados a los usos de los diferentes sistemas de IA, por lo cual comedidamente sugerimos revisar la posibilidad de dejar esta clasificación para la reglamentación de la ley, indicando que dicha clasificación debe atender los principios y valores de que trata el presente proyecto.

Ahora bien, no obstante recomendar que la clasificación de riesgos no debe hacer parte del proyecto de Ley, sino que debería hacer parte de la reglamentación, a continuación, se presentan algunas observaciones específicas al artículo propuesto.

En la definición de alto riesgo se observa que solo se hace alusión a las actividades que son susceptibles de automatización, excluyendo aquellos sistemas de IA que están orientados a realizar predicciones o tomar decisiones a través del aprendizaje continuo, lo que puede generar vacíos en el momento de la aplicación.

Frente a la definición de riesgo limitado solo se incluyen los *chatbots* o robots convencionales, desconociendo que los sistemas de IA tienen la capacidad, no solo de realizar tareas repetitivas, sino que también a través del aprendizaje automático desarrollan nuevas capacidades o generan contenido. Por lo cual, según la definición propuesta, no es claro si los sistemas de aprendizaje automático harían parte de esta categoría de riesgo.

- **ARTÍCULO 9. TRANSPARENCIA EN EL USO DE LA INTELIGENCIA ARTIFICIAL.** Los productores y proveedores que desarrollen, ofrezcan y pongan en funcionamiento y los usuarios que empleen sistemas de inteligencia artificial de riesgo alto y limitado deberán publicar una evaluación sobre los riesgos y el impacto que pudieran llegar a sufrir los derechos humanos y fundamentales, antes de desplegar dichos sistemas. De impacto en la privacidad, que debe incluir por lo menos los siguientes criterios:
 - a. Una descripción detallada de las operaciones de tratamiento de datos personales que involucre el desarrollo de la inteligencia artificial.
 - b. Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales.
 - c. Las medidas previas para afrontar los riesgos.

Comentario:

De acuerdo con el artículo propuesto, se establece que la publicación de la evaluación de riesgos e impacto debe ser realizada para todos los sistemas de inteligencia artificial de riesgo alto y limitado, por lo que teniendo en consideración la normatividad adoptada en la Unión Europea, se recomienda que la obligación de publicación y entrega al Ministerio TIC (obligación definida en el párrafo 2) solo sea aplicable a los sistemas categorizados como de riesgo alto.

Adicionalmente, en el artículo propuesto se define que la publicación de la evaluación de los riesgos y el impacto se realice antes de desplegar el sistema de IA, ante lo cual se recomienda que dicha obligación quede supeditada a la finalización del despliegue. Dado que es en este punto donde el sistema se lleva desde el entorno de desarrollo al entorno de producción, y se realiza el monitoreo del modelo, para detectar y corregir posibles errores. Asegurando así que el modelo esté listo para su uso.

- **ARTÍCULO 11. ALFABETIZACIÓN DIGITAL.** El Ministerio de Educación Nacional en coordinación con el Ministerio de tecnologías de la información y las comunicaciones

formularán, dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente ley, políticas de alfabetización digital con énfasis en el uso responsable y ético de los sistemas y/o programas de inteligencia artificial. Estas políticas se implementarán para estudiantes de educación básica, media y superior, con el único fin de formar integralmente a los jóvenes en el uso responsable y productivo de sistema de inteligencia artificial.

Comentario:

Es necesario que se aborde la alfabetización mediática, ya que dicha alfabetización busca la definición de estrategias y directrices para empoderar a los estudiantes para que puedan tomar decisiones informadas, reconocer sesgos, enfrentar la desinformación, evaluar críticamente la información y crear contenido de manera responsable.

Por lo consiguiente, la alfabetización digital y la alfabetización mediática para estudiantes, si bien debe estar en cabeza del Ministerio de Educación y ser apoyada por el Ministerio TIC, también podría ser apoyada por la Sesión de Contenidos Audiovisuales de la Comisión de Regulación de Comunicaciones.

- **ARTÍCULO 14. RESPONSABILIDAD LEGAL EN MATERIA DE INTELIGENCIA ARTIFICIAL y ARTÍCULO 15. RESPONSABILIDAD SOCIO AMBIENTAL**

[...] **PARÁGRAFO 1.** Los responsables legales en materia de inteligencia artificial deberán informar y advertir a las autoridades competentes sobre los potenciales riesgos, deficiencias e incidentes graves presentados en el manejo y gestión de esta.

Comentario:

En el parágrafo 1 de los artículos 14 y 15 se establece una obligación que le asiste a los «responsables legales en materia de inteligencia artificial», no obstante, el artículo de definiciones no se establece dicho sujeto, por lo cual se recomienda incluir la definición en el artículo 3 del Proyecto de ley. Así mismo, se recomienda identificar quiénes son las entidades competentes para recibir el reporte de los potenciales peligros de los sistemas de IA tanto en materia legal como en materia ambiental.

- **ARTÍCULO 19. PLATAFORMA DE CERTIFICACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL.** Los productores y proveedores que desarrollen, ofrezcan e instalen inteligencia artificial que desarrollen sistemas de inteligencia artificial deberán registrar sus modelos en la plataforma de certificación que administrará el Ministerio de las Tecnologías de la Información y Comunicaciones quien certificará que se encuentren ajustados a derechos humanos y fundamentales y autorizará su viabilidad.

Los productores nacionales e internacionales que usen sistemas de inteligencia artificial en Colombia deberán rendir un informe anual ante la Superintendencia de Industria y Comercio en el que demuestran, como mínimo, el cumplimiento de las obligaciones señaladas en la presente ley. La autoridad competente deberá constatar el efectivo cumplimiento de las obligaciones y certificará que se encuentra ajustado a los estándares de esta ley.

Comentario:

En el artículo propuesto se establece que corresponde al Ministerio TIC administrar la Plataforma de Certificación de Sistemas de Inteligencia Artificial, pero en el artículo 16 del Proyecto de Ley, el cual modifica el artículo 19 de la Ley 1581 de 2012, se establece como función de la Superintendencia de Industria y Comercio la administración de la Plataforma de Certificación de Sistemas de Inteligencia Artificial. Así las cosas, no es claro cuál es la entidad que estará encargada de la administración de esta, para así no duplicar funciones ni crear la obligación de un registro ante la plataforma del MinTIC, y otro ante la plataforma de la SIC

No obstante, la falta de claridad indicada en el párrafo anterior, se recomienda eliminar la obligación de registro para el proceso de certificación, toda vez que dicha obligación establecería una carga que podría ir en contra de la innovación.

Adicionalmente, según lo dispuesto en el citado artículo el registro que se debe realizar es de los modelos de inteligencia artificial y no de los sistemas, por lo cual dado que un sistema puede incluir múltiples modelos que interactúan entre sí, no es claro si la autorización de viabilidad de que trata el artículo obedecerá al funcionamiento de los modelos o de los sistemas, por lo cual recomendamos aclarar sobre qué bien versa la autorización y cuál sería el proceso para aquellos modelos abiertos.

Sin perjuicio de las observaciones relacionadas para el artículo propuesto, comedidamente sugerimos revisar el impacto que tendría la obligación de registrar todos los modelos de inteligencia artificial que se desarrollen, ofrezcan e instalen en el país; dado que dicha carga podría desincentivar el uso y despliegue de sistemas de inteligencia artificial en el país, generando una gran brecha con otros países de la región.

En los anteriores términos damos respuesta a su solicitud y quedamos atentos a realizar cualquier aclaración al respecto.

Cordialmente,

LINA MARIA DUQUE DEL VECCHIO

Directora Ejecutiva

Proyectado por: Diana Morales / David Agudelo

Aprobado por: Zoila Vargas