

Bogotá D.C., 25 de mayo de 2026

Honorables Congresistas

PEDRO FLOREZ PORRAS

GERSON LISIMACO MONTAÑO ARIZALA

Comisión Sexta

CONGRESO DE LA REPÚBLICA

La Ciudad

Asunto: Comentarios al Informe de Ponencia Positiva para Primer Debate al Proyecto de Ley 043 de 2025 Senado y 324 de 2025 Cámara “Por medio del cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético, responsable, competitivo e innovador, y se dictan otras disposiciones”

Honorables Congresistas,

Comienzo por extenderles nuestros más cordiales saludos de parte de la Cámara Colombiana de Informática y Telecomunicaciones – CCIT, organización gremial que agrupa a las más importantes empresas del sector de las Tecnologías de la Información y las Comunicaciones de Colombia. En ese sentido, hemos venido trabajando en el país por más de 33 años contribuyendo activamente desde el Sector TIC a la eliminación de barreras para la evolución tecnológica, promoviendo el cierre de la brecha digital, la democratización y la masificación de las TIC, así como el acceso de todos los ciudadanos a la sociedad y economía del conocimiento.

En esta ocasión nos dirigimos a Ustedes con el fin de presentar nuestros comentarios al Informe de Ponencia Positiva para Primer Debate al Proyecto de Ley 043 de 2025 Senado y 324 de 2025 Cámara "Por medio del cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético, responsable, competitivo e innovador, y se dictan otras disposiciones". En ese sentido, presentamos las siguientes observaciones.

1. Comentarios generales

1.1. Críticas y estado de implementación de la normativa europea

La Unión Europea fue pionera en proponer, en 2021, el primer marco regulatorio integral sobre IA, estructurado a partir de un esquema de clasificación por niveles de riesgo que el presente Proyecto de Ley busca replicar. Sin embargo, dicho modelo aún no ha entrado plenamente en vigor y la propia Comisión Europea ha promovido el aplazamiento de su aplicación completa hasta 2027, además de encontrarse actualmente en un proceso de revisión y negociación de modificaciones.

Lo anterior obedece, entre otras razones, a la que la concepción inicial normativa europea no contempló adecuadamente el desarrollo acelerado de los grandes modelos de lenguaje ni casos

de uso general. Asimismo, la coexistencia de múltiples reglamentaciones ha evidenciado tensiones con la naturaleza dinámica y evolutiva de la IA.

En la práctica, esta situación ha generado situaciones de inseguridad jurídica que han dificultado la planeación estratégica de las empresas y aumentado significativamente los costos regulatorios. En particular, las empresas se han visto obligadas a destinar recursos considerables a evaluaciones de riesgo, trazabilidad algorítmica, auditorías de datos y protocolos de transparencia y responsabilidad, sin contar con claridad suficiente sobre la suficiencia de dichas inversiones.

Este efecto ha resultado especialmente regresivo para las pequeñas y medianas empresas (Pymes), que carecen de las capacidades financieras y operativas de las grandes compañías para asumir estos costos. Como consecuencia, una regulación concebida inicialmente para democratizar la confianza en la IA ha terminado profundizando las asimetrías existentes y generando efectos inhibidores sobre la innovación, situación que explica, la decisión de posponer su aplicación.¹

En ese contexto, resulta problemático que Colombia avance hacia la adopción de un marco regulatorio inspirado en el esquema europeo sin considerar que dicho modelo aún enfrenta dificultades de implementación en su propia jurisdicción, así como cuestionamientos relacionados con su enfoque incorrecto, sus elevados costos, su complejidad operativa y sus efectos inhibidores sobre la innovación.

Esta preocupación adquiere especial relevancia si se tiene en cuenta que el entorno colombiano presenta limitaciones estructurales significativamente mayores en materia de inversión, infraestructura tecnológica y capacidades avanzadas en ciencia y tecnología. De hecho, el Documento CONPES 4144 de 2025 reconoce que:

“A nivel empresarial, se encuentran bajos niveles de inversión y financiación en tecnología e innovación para la IA. La inversión privada en Inteligencia artificial en Colombia para 2022 fue de USD 35 millones, ocupando el sexto puesto luego de países como Brasil (USD 769 millones), México (USD 259 millones) y Chile (USD 80 millones) (Emerging Technology Observatory, 2024). En línea con lo anterior, para 2023 Colombia presentó un flujo de financiación de las empresas en IA de USD 1,7 millones de dólares, mientras que países como Chile y Brasil presentan flujos de USD 9,3 y USD 6 millones de dólares respectivamente. (Tortoise Media, 2023). Finalmente, el informe de los Diálogos Regionales sobre Inteligencia Artificial también revela que solo el 17.3 % de los participantes indicaron que sus instituciones contaban con algún tipo de financiamiento para proyectos de IA.”²

¹ Supantha Mukherjee y Bart H. Meijer, “EU to delay ‘high risk’ AI rules until 2027 after Big Tech pushback”, Reuters, 19 de noviembre de 2025, disponible en: <https://www.reuters.com/sustainability/boards-policy-regulation/eu-delay-high-risk-ai-rules-until-2027-after-big-tech-pushback-2025-11-19>

²Departamento Nacional de Planeación(2025). CONPES 4144 — Política Nacional de Inteligencia Artificial 2025-2035”. Disponible en: <file:///mnt/data/4144.pdf>

En consecuencia, la adopción de un esquema regulatorio complejo y altamente exigente podría traducirse en una carga regulatoria desproporcionada, afectando la competitividad y desincentivando el desarrollo tecnológico en un sector estratégico para el futuro económico y social del país. Por estas razones, cualquier iniciativa de regulación de IA en Colombia debe partir de diagnósticos realistas así como de procesos amplios de deliberación y de una aproximación gradual, flexible y contextualizada, que permita promover el desarrollo de la tecnología sin convertir la regulación en una barrera para la innovación sino un habilitador del sector tecnológico.

1.2. Afectación desproporcionada a las Pymes

Las Pymes representan más del 91,8% del tejido empresarial colombiano y generan aproximadamente el 80% del empleo formal en el país³. No obstante, la adopción de tecnologías de IA es del 2,4% de las Pymes y el 0,7% de las microempresas.⁴

Esta situación resulta particularmente relevante si se considera que la IA puede convertirse en un mecanismo fundamental para el crecimiento económico de las pymes, permitiéndoles competir en condiciones más equitativas frente a actores consolidados. A través de la automatización, análisis de datos y optimización de procesos, la IA tiene el potencial de reducir costos operativos, mejorar la productividad, ampliar la capacidad de atención al cliente y facilitar el acceso a nuevos mercados sin requerir inversiones de gran escala⁵. En otras palabras, la IA constituye una herramienta habilitadora de la transformación digital del tejido empresarial colombiano.

Sin embargo, las obligaciones previstas en el Proyecto de Ley impactan de manera desproporcionada a este segmento empresarial. A diferencia de las grandes compañías, las Pymes no cuentan con equipos jurídicos, técnicos y financieros especializados que les permitan implementar adecuadamente obligaciones complejas como evaluaciones de riesgo o sistemas de transparencia. Cada uno de estos requisitos implica inversiones que exceden su capacidad operativa y que podrían obligarlas a desviar recursos esenciales destinados a innovación, expansión y generación de empleo.

En consecuencia, la regulación propuesta podría convertirse en una barrera adicional para la apropiación de IA por parte de las Pymes, limitando su competitividad y excluyéndolo del ecosistema digital. Esta preocupación coincide con lo señalado por el Global AI Adoption Index 2022 de IBM, según el cual la baja adopción empresarial de IA, particularmente en pequeñas empresas, se explica principalmente por el limitado conocimiento sobre IA (26%), la ausencia de

³La Nota Económica. “En Colombia el 91,8 % de las empresas son PyMEs”, disponible en: <https://lanotaeconomica.com.co/movidas-empresarial/en-colombia-el-918-de-las-empresas-son-pymes/>

⁴ Departamento Nacional de Planeación (2025). CONPES 4144 — Política Nacional de Inteligencia Artificial 2025-2035”. Disponible en: <file:///mnt/data/4144.pdf>

⁵IFT Transformación Digital (2024). Inteligencia Artificial en las PYMES: Ventajas, Riesgos”. Disponible en: <https://www.ift.org.mx/transformacion-digital/blog/inteligencia-artificial-en-las-pymes-ventajas-riesgos>

herramientas y plataformas para el desarrollo de IA (24%) y los altos costos de implementación (21%)⁶.

De aprobarse la iniciativa sin considerar estas limitaciones, el resultado podría ser contrario al objetivo de promover la innovación. En lugar de facilitar la adopción de IA, el proyecto podría convertirla en una tecnología inaccesible para las Pymes debido a las cargas financieras y regulatorias asociadas a su cumplimiento.

1.3. Freno a la innovación

Aunque el Proyecto de Ley busca fortalecer la seguridad, la transparencia y la confianza en el uso de la IA, su diseño podría producir efectos contrarios a los perseguidos. En particular, la iniciativa anticipa obligaciones regulatorias complejas antes de que el ecosistema colombiano de innovación haya desarrollado las capacidades necesarias para cumplirlas adecuadamente. El CONPES 4144 de 2025 reconoce que:

“en Colombia, las capacidades para la innovación mediante la incorporación de sistemas de Inteligencia Artificial (IA) son limitadas, afectando especialmente a las micro y pequeñas empresas. Durante 2020, solo el 12 % de las empresas colombianas implementaron procesos de IA, en su mayoría en grandes empresas. En este mismo sentido, en promedio el 60 % de las empresas que implementaron procesos de innovación en IA optaron por tercerizar el diseño, la operación y el mantenimiento de soluciones. Finalmente, para las empresas que no desarrollaron o utilizaron alguna herramienta o aplicación de IA, se determinó que el 48 % no hicieron uso de dichas tecnologías debido a que las empresas desconocen las funcionalidades de los software o soluciones tecnológicas disponibles para la solución de problemáticas al interior de la organización.”⁷.

Este contexto, evidencia que el uso e innovación de IA en Colombia aun es limitado. En consecuencia, la aprobación de un marco regulatorio altamente exigente podría detener o limitar los procesos de innovación con el fin de adaptar desarrollos tecnológicos a una normativa cuya evolución probablemente será más lenta que la de la propia tecnología que se pretende regular.⁸

A ello se suma que la IA constituye una tecnología en permanente evolución y mejora, por lo que tratarla como un producto estático, como lo prevé el Proyecto de Ley, implicaría imponer límites incompatibles con la velocidad del cambio tecnológico. Esta desfase entre la naturaleza dinámica de la IA y la rigidez normativa produce tensiones operativas, incrementa la inseguridad jurídica y

⁶ Departamento Nacional de Planeación(2025). CONPES 4144 — Política Nacional de Inteligencia Artificial 2025-2035”. Disponible en: <file:///mnt/data/4144.pdf>

⁷ Ibidem.

⁸ IESE Insight. Artificial Intelligence in Europe: innovation, regulation and the risk of over-regulation. Disponible en: <https://www.iese.edu/insight/articles/artificial-intelligence-europe-innovation-regulation/>

genera un entorno empresarial en el que el riesgo del incumplimiento y sanción termina prevaleciendo sobre los incentivos para innovar.

En este escenario, una regulación concebida para proteger derechos y generar confianza podría terminar afectando negativamente la adopción y el desarrollo de IA en Colombia. En lugar de consolidarse como un motor de competitividad, la regulación correría el riesgo de convertirse en una barrera para el desarrollo tecnológico y para el aprovechamiento de una herramienta con capacidad de redefinir sectores completos de la economía colombiana.

2. Comentarios particulares

2.1. Comentarios respecto al artículo 2 “Ámbito de aplicación”

El ámbito de aplicación propuesto en el artículo 2 del Proyecto de Ley resulta excesivamente amplio, en la medida en que permite que prácticamente cualquier actor, tecnología o actividad digital pueda quedar sometido a la regulación, incluso sin contar con presencia en Colombia. Esta aproximación desconoce el principio de territorialidad de la ley, respecto del cual la Corte Constitucional ha señalado que:

“El principio de la territorialidad de la ley es consustancial con la soberanía que ejercen los Estados dentro de su territorio; de este modo cada Estado puede expedir normas y hacerlas aplicar dentro de los confines de su territorio.”⁹

En este contexto, la redacción propuesta extiende la jurisdicción colombiana más allá de límites razonables, pues bastaría con que un sistema produzca algún efecto económico, utilice datos de origen colombiano o dependa parcialmente de la infraestructura localizada en el país para que una empresa extranjera quede sometida al régimen, aun cuando no opere ni comercialice directamente sus servicios en Colombia o carezca de control efectivo sobre la operación del sistema dentro del territorio nacional.

Adicionalmente, el artículo establece que *“para todos los efectos de esta ley, las personas o entidades que cumplan con alguno de los supuestos anteriores serán consideradas “Responsables de IA”*”. Esta redacción resulta problemática porque equipara actores que desarrollan tecnología, a quienes la integran y a quienes simplemente la utilizan. En consecuencia, la disposición impone obligaciones idénticas tanto a quienes tienen control total sobre un sistema y a quienes únicamente acceden a una herramienta provista por terceros.

Esta ausencia de diferenciación genera un escenario de responsabilidad indeseable, en los que empresas colombianas podrían enfrentar sanciones derivadas de decisiones o funcionalidades asociados a sistemas sobre los cuales no tienen capacidad técnica ni contractual de intervención.

⁹ Corte Constitucional. Sentencia C-249 de 2004. M.P. Jaime Araújo Rentería

Lejos de incentivar el uso y desarrollo de IA, esta imprecisión regulatoria puede convertirse en un desincentivo significativo para la adopción de tecnologías de IA en el país.

Finalmente, el artículo emplea conceptos amplios e indeterminados, tales como “efectos jurídicos, económicos, sociales o ambientales”, sin establecer criterios objetivos que permitan determinar en qué circunstancias un sistema queda cubierto por la ley ni precisar el alcance concreto de dichos efectos. Esta ambigüedad genera inseguridad jurídica y amplía los márgenes de discrecionalidad por parte del operador jurídico, encargado de interpretar y aplicar la regulación.

2.2. Comentarios respecto al artículo 3 “Principios rectores para el desarrollo y uso de la inteligencia artificial”

2.2.1. Comentarios frente al numeral 3.3.

El numeral establece la obligación de realizar evaluaciones de impacto social, cultural, económico y ambiental para cualquier sistema de IA, sin incorporar excepciones o criterios de proporcionalidad. Esta aproximación desconoce que no todos los sistemas de IA generan efectos económicos, sociales o ambientales significativos.

En consecuencia, exigir evaluaciones de impacto incluso para herramientas triviales, sistemas internos de automatización o modelos utilizados sin interacción pública convierte la regulación en una carga desproporcionada que limita la adopción tecnológica sin generar beneficios reales en materia de protección de derechos. En la práctica, la disposición termina transformando la innovación en un procedimiento administrativo previo, inhibiendo el desarrollo y elevando los costos de entrada para nuevos actores.

Adicionalmente, la obligación de exigir impactos a corto, mediano y largo plazo introduce una exigencia prospectiva imposible de verificar, desde el punto de vista técnico, dado que actualmente no existen herramientas que permitan prever con suficiente certeza los efectos futuros de tecnologías caracterizadas por su evolución constante.

La obligación propuesta confunde el control efectivo sobre un sistema de IA con el simple uso o integración tecnológica. Un usuario que consume una API o contrata servicios en la nube no tiene acceso a algoritmos, datos o procesos técnicos internos, por lo que carece de capacidad real para evaluar impactos que dependen exclusivamente del desarrollador original. En ese sentido, trasladar obligaciones imposibles de cumplir a actores sin control efectivo sobre la tecnología genera riesgos regulatorios innecesarios y desincentiva tanto el uso como el desarrollo de capacidades locales en IA.

Finalmente, el numeral 3.3. presenta inconsistencias con el artículo 6 del Proyecto, el cual establece que los sistemas de IA que no sean considerados de alto riesgo estarán exentos de evaluaciones de impacto, mientras que el numeral 3.3. la impone de manera general para todos

los actores vinculados al ciclo de vida de la IA. Esta contradicción normativa genera inseguridad jurídica respecto del verdadero alcance de la obligación.

2.2.2. Comentarios respecto al numeral 3.5.

En relación con la capacidad de verificación, auditoría y cuestionamiento prevista en este numeral, resulta indispensable garantizar expresamente que su aplicación no implique el desconocimiento de derechos e intereses legítimos de los actores privados, particularmente aquellos relacionados con secretos empresariales, propiedad intelectual y seguridad de los sistemas.

Lo anterior, en la medida en que ello no puede traducirse en obligaciones de divulgación técnica que impliquen revelar documentación, metodologías, datos internos protegidos por secretos empresariales o derechos de propiedad intelectual. La ausencia de salvaguardas, podría generar una desventaja competitiva al exponer información diferenciadora en el mercado que podría ser fácilmente replicada por competidores. La ausencia de salvaguardas podría erosionar la competitividad empresarial y desincentivar la innovación.

En ese sentido, debe tenerse presente que el artículo 333 de la Constitución Política protege la libertad económica y la iniciativa privada. Por tanto, no resulta admisible imponer obligaciones de divulgación de documentación técnica, metodologías o datos internos, en la medida en que ello podría afectar el ejercicio legítimo de la actividad económica.

En consecuencia, sugerimos ajustar la redacción del artículo con el fin de armonizar los principios de transparencia y trazabilidad con la protección de los secretos empresariales, la propiedad intelectual y la libertad económica, garantizando que cualquier exigencia de verificación se implemente con pleno respeto por los derechos de los actores privados.

2.2.3. Comentarios respecto al numeral 3.6.

Este numeral incurre en una generalización problemática al asumir que toda aplicación de IA debe generar un impacto transformador sobre desafíos públicos, productivos, sociales o ambientales. Esta aproximación desconoce que la IA no constituye un conjunto homogéneo de tecnologías estratégicas y que existen herramientas triviales, utilitarias o de uso cotidiano cuya finalidad no consiste en resolver problemas estructurales, sino en automatizar procesos menores, realizar tareas simples o mejorar experiencias de usuario.

En consecuencia, exigir que cualquier uso de IA genere soluciones transformadoras desconoce esta diversidad y sobredimensiona las obligaciones regulatorias. Esta visión rígida puede terminar afectando especialmente el desarrollo de aplicaciones sencillas, experimentales o de nicho, que constituyen el punto de entrada para la innovación temprana y el desarrollo empresarial en ecosistemas emergentes como el colombiano.

2.2.4. Comentarios respecto al numeral 3.9.

Respecto de este numeral, se establece un estándar de responsabilidad excesivamente amplio al imponer a los desarrolladores la obligación de evitar cualquier perjuicio derivado del uso de sistemas de IA, incluso en contextos sobre los cuales no tienen control efectivo. Esta aproximación desconoce que la IA opera en contextos completos, interactúa con datos que no siempre son verificables y puede producirse efectos indirectos e imprevisibles.

En consecuencia, pretender que los desarrolladores eliminen por completo cualquier efecto adverso o riesgo transforma la innovación en una actividad de alto riesgo jurídico y económico. Además la disposición no diferencia entre daño intencional, negligencia y efectos no atribuibles al desarrollador, lo que podría dar lugar a sanciones incluso cuando el actor haya actuado con diligencia conforme a estándares técnicos razonables.

La responsabilidad en materia de IA debe centrarse en conductas dolosas o negligentes claramente demostrables, y no sobre un estándar absoluto e imposible que desconoce la naturaleza de la IA. De mantenerse la redacción actual, la disposición podría desalentar la investigación, elevar los costos de desarrollo y afectar negativamente la competitividad del ecosistema colombiano.

2.3. Comentarios respecto al artículo 4 “Definiciones”

2.3.1. Comentarios respecto al numeral 4.1. “Definición IA”

La definición de IA propuesta en el numeral resulta problemática en la medida en que atribuye a estas tecnologías capacidades que no poseen, generando confusiones conceptuales con importantes consecuencias jurídicas. En particular, al señalar que la IA “percibe su entorno”, “razona”, “aprende de la experiencia” o “toma decisiones de manera autónoma”, la disposición supone un entendimiento antropomorfizado y técnicamente inexacta de la tecnología¹⁰, al conferirle características propias de los seres humanos.

La IA no comprende, percibe ni razona; simplemente procesa datos y patrones estadísticos conforme a instrucciones desarrollados por personas. En consecuencia, asignarle facultades cognitivas o autonomía puede conducir erróneamente a considerar que la responsabilidad sobre decisiones recae en la tecnología.

Adicionalmente, la definición propuesta es tan amplia que podría abarcar prácticamente cualquier sistema informático que procese datos, diluyendo el concepto de IA e impidiendo delimitar con claridad que tecnologías quedarían sometidas a la regulación. Esta aproximación ignora los estándares internacionales, los cuales evitan describir la IA como un ente capaz de razonar o

¹⁰ Adriana Placani, “Anthropomorphism in AI: hype and fallacy”, *AI and Ethics* 4, no. 3 (2024): 691-698, doi:10.1007/s43681-024-00419-4.

tomar decisiones, y por el contrario, se limitan a caracterizarlo como un conjunto de métodos computacionales diseñados para ejecutar tareas específicas basadas en modelos matemáticos y estadísticos.

En consecuencia, la regulación colombiana no debería partir de definiciones que sobrepasan las capacidades reales de la tecnología ni trasladan atributos humanos inexistentes. Por lo anterior, sugerimos ajustar la definición para alinearla con la evidencia técnica y con los marcos regulatorios internacionales que describen a la IA de manera funcional, verificable y libre de atribuciones cognitivas que no corresponden con la realidad.

2.3.2. Comentarios respecto al numeral 4.2. “Definición Sistema de IA”

La definición propuesta resulta problemática en la medida en que sugiere que estos sistemas “perciben” su entorno, “abstraen” información y derivan acciones mediante “inferencias lógicas”, dando la impresión que poseen capacidades cognitivas análogas a las humanas.

Esta formulación desconoce que los sistemas de IA no comprenden, no razonan, no tienen intención ni conciencia. Su funcionamiento consiste en procesar datos y aplicar algoritmos estadísticos entrenados para identificar patrones y generar respuestas probabilísticas. Incluso los modelos más avanzados no toman decisiones ni ejecutan acciones con criterios propios, sino que calculan la salida más probable a partir de una entrada.

Presentar estas operaciones como procesos de percepción o razonamiento introduce una carga antropomórfica que distorsiona la verdadera naturaleza de la tecnología¹¹ y puede derivar en obligaciones jurídicas inaplicables, al atribuir a la IA capacidades inexistentes y responsabilidades que corresponden exclusivamente a los actores humanos involucrados en su diseño, entrenamiento, implementación y supervisión.

2.3.3. Comentarios respecto al numeral 4.8. “Definición Responsable de IA”

El concepto de “responsable de IA” resulta excesivamente amplio, en la medida en que convierte en sujetos obligados a todos los actores que participan en cualquier etapa del ciclo de vida de un sistema, sin diferenciar entre quienes tienen poder de decisión y control y quienes son simplemente usuarios.

Bajo esta definición, la responsabilidad no se asigna a quien efectivamente ejerce control sobre el diseño, operación o despliegue del sistema, sino a cualquier actor que “participe” incluso cuando no tenga acceso técnico, capacidad de supervisión o posibilidad real de mitigar riesgos.

Esta amplitud genera un escenario de incertidumbre jurídica y riesgos regulatorios imposibles de gestionar, especialmente para Pymes, implementadores y usuarios finales, quienes podrían verse

¹¹ Ibidem.

expuestos a exigencias legales desproporcionadas respecto de procesos o decisiones que escapen completamente de su control.

2.3.4. Comentarios respecto al numeral 4.9. “Definición Desarrollador de IA”

La definición propuesta en el numeral 4.9 establece que el desarrollador “*será responsable por la calidad técnica, la robustez, la mitigación de sesgos y la transparencia sobre capacidades y limitaciones del sistema*”. En particular, la transparencia sobre capacidades y limitaciones de un sistema de IA deben exigirse únicamente en la medida en que ello sea técnicamente posible y no implique la revelación de secretos empresariales o propiedad intelectual, los cuales constituyen el núcleo de valor competitivo de los desarrolladores.

En consecuencia, el régimen de responsabilidad del desarrollador debe armonizarse con garantías explícitas de protección de estos derechos, asegurando un equilibrio adecuado entre la debida diligencia técnica y la preservación de activos estratégicos indispensables para el crecimiento del ecosistema de IA.

2.3.5. Comentarios respecto al numeral 4.13. “Definición Transparencia”

La definición de transparencia prevista en el numeral 4.13 resulta excesivamente amplia y podría interpretarse en el sentido de exigir acceso irrestricto a la información sobre el diseño y funcionamiento interno de los sistemas de IA por parte de usuarios y autoridades, sin establecer salvaguardas suficientes para proteger información sensible.

Si bien la transparencia constituye un principio fundamental para promover confianza y asegurar el uso responsable de la tecnología, ello no puede traducirse en obligaciones de divulgación absoluta respecto de modelos, arquitecturas, parámetros, código fuente o elementos protegidos por secretos empresariales, propiedad intelectual o medidas de seguridad. Una interpretación de esta naturaleza obligaría, en la práctica, a las empresas a revelar sus activos estratégicos afectando negativamente su ventaja competitiva e inhibiendo la innovación en el sector.

Por esta razón, la transparencia debe entenderse como la provisión de información pertinente, verificable y contextualizada, únicamente en la medida en que ello sea técnica y jurídicamente posible, sin comprometer derechos adquiridos ni exponer componentes confidenciales cuya divulgación vulneraría la Constitución Política y la legislación vigente, así como desincentivaría el desarrollo tecnológico.

Asimismo, la obligación de transparencia debe modularse según el rol específico del actor y el nivel de riesgo del sistema, de manera que la información exigida refleje las capacidades reales y limitaciones técnica de cada herramienta así como sus condiciones generales de funcionamiento. Imponer obligaciones uniformes para todos los sistemas y actores desconoce la diversidad del ecosistema tecnológico y puede afectar negativamente la innovación, especialmente en sectores emergentes y empresas de menor escala.

2.3.6. Comentarios respecto al numeral 4.14. “Definición Explicabilidad”

La definición de explicabilidad presenta problemas conceptuales y operativos relevantes. En primer lugar, al exigir información comprensible para las “personas afectadas”, introduce una categoría ambigua que no delimita claramente quien debe considerarse afectado ni bajo que circunstancias, lo que puede dar lugar a interpretaciones expansivas y obligaciones desproporcionadas.

Adicionalmente, la explicabilidad no puede exigirse de manera uniforme para todos los sistemas, pues su alcance debe responder al nivel de riesgo asociado al caso de uso concreto. Exigir explicaciones respecto de procesos internos incluso para sistemas de bajo riesgo desconoce diferencias técnicas y genera cargas regulatorias innecesarias sin beneficios reales en materia de protección de derechos.

La definición también sugiere que la explicabilidad implica revelar procesos y razonamientos técnicos de los sistemas, desconociendo tanto la naturaleza estadística de la IA como la necesidad de proteger secretos empresariales y propiedad intelectual. Los sistemas de IA no razonan en sentido humano, sino que operan mediante cálculos probabilísticos y modelos estadísticos basados en inferencias matemáticas. Por ello, solicitar que se expliquen supuestos razonamientos algorítmicos conlleva un riesgo regulatorio, pues se exige a los sistemas una capacidad que no poseen y se abre la puerta a demandas para revelar información confidencial o detalles técnicos cuyo acceso no es necesario ni proporcional para garantizar la rendición de cuentas.

En consecuencia, la definición termina confundiendo la obligación de proporcionar explicaciones útiles y contextualizadas con una expectativa de transparencia técnica absoluta, lo que resulta jurídicamente inseguro y técnicamente inviable. La explicabilidad debe formularse como un principio proporcional al riesgo, orientado a permitir la comprensión de los factores relevantes que inciden en los resultados, sin exigir la divulgación de arquitecturas, parámetros, código fuente o mecanismos internos que no constituyen razonamientos, sino operaciones estadísticas complejas.

2.3.7. Comentarios respecto al numeral 4.20. “Definición Evaluación de impacto de IA”

La definición propuesta para evaluación de impacto de IA resulta imprecisa al partir del supuesto que dicha evaluación debe centrarse en “posibles efectos adversos”, cuando en la práctica regulatoria en materia de IA se basan en gestión de riesgos y no en la identificación de daños o potenciales efectos negativos específicos.

La referencia de efectos adversos supone que estos ya existen o son previsibles, lo que desplaza la lógica preventiva de la regulación hacia una lógica reactiva que sobredimensiona la carga probatoria del evaluador, lo que podría implicar exigir la demostración de daños difíciles de identificar en etapas tempranas del ciclo de vida del sistema.

Por el contrario, un enfoque basado en riesgos permite anticipar escenarios y establecer niveles de intervención proporcionales, así como adoptar medidas graduales sin asumir que toda aplicación de IA es inherentemente dañina.

En consecuencia, mantener la referencia a “efectos adversos” podría confundir categorías técnicas con juicios de valor y generar inseguridad jurídica al exigir evaluaciones sobre consecuencias difíciles de delimitar y dependientes del contexto del uso, del tipo de datos y de la interacción humana. Las evaluaciones de impacto deben orientarse a la identificación y gestión de riesgos razonablemente previsibles y no a la catalogación de daños hipotéticos o indeterminados.

2.3.8. Comentarios respecto al numeral 4.23. “Definición Responsabilidad Civil de la IA”

La definición propuesta omite un elemento esencial para garantizar la seguridad jurídica. En particular, la responsabilidad en materia de IA no puede fundarse únicamente en resultados imprevisibles o en la sola ocurrencia del daño, sino en conductas dolosas o negligentes demostrables y atribuibles a quien tenía capacidad real de evitarlo.

La tecnología, por sí misma, no actúa ni toma decisiones autónomas. En consecuencia, la imputación de responsabilidad debe recaer exclusivamente sobre los sujetos que ejercen control efectivo sobre el diseño, despliegue o uso de la herramienta, atendiendo al régimen de responsabilidad civil colombiano.

Por estas razones, una regulación adecuada debe estructurar un régimen de responsabilidad coherente con los principios del derecho civil colombiano, basado en la culpa, el daño y el nexo causal, y no en modelos de responsabilidad objetiva que trasladan riesgos excesivos a actores sin capacidad efectiva de gestión, afectando la innovación y generando incertidumbre normativa.

2.4. Comentarios respecto al artículo 5 “Clasificación de riesgos”

En primer lugar, la categoría de “Sistemas de Riesgo Crítico” incorpora expresiones indeterminadas como “contradecir de manera sustancial los derechos fundamentales”, formulación que no resulta adecuada desde el punto de vista constitucional. Los derechos fundamentales no se “contradicen”, sino que pueden verse afectados de manera negativa y grave en su núcleo esencial. En consecuencia, la terminología empleada no se ajusta al lenguaje constitucional sobre el alcance de los derechos fundamentales.

Adicionalmente, la indeterminación respecto a cuando existe una afectación sustancial abre amplios márgenes de interpretación discrecional y podría conducir a la prohibición de sistemas cuyos efectos no constituyen daños graves o verificables.

Por otra parte, el artículo otorga a la autoridad nacional competente amplias facultades reglamentarias, incluyendo la posibilidad de “revisar y actualizar periódicamente la clasificación”

de los riesgos sin establecer parámetros legales claros ni límites materiales a dicha intervención. Esta habilitación resulta problemática en la medida en que traslada al ejecutivo competencias propias del legislador, desconociendo el artículo 150 de la Constitución Política, que reserva al Congreso la potestad de hacer las leyes y delinear su contenido esencial.

Si bien el numeral 11 del artículo 189 de la Constitución reconoce la facultad reglamentaria del Ejecutivo, esta facultad no le permite rediseñar, modificar ni legislar. Al respecto, la Corte Constitucional ha establecido:

“Sin embargo, dicha facultad reglamentaria no es absoluta pues ella se ejerce en la medida en que exista la ley. Ley que se convierte en su límite. Es por ello que cuando el Ejecutivo reglamenta la ley no puede ir más allá de lo que ella prevé, ni de las pautas generales que señala. Es bajo este entendimiento, que la facultad reglamentaria del Ejecutivo puede ser en algunos casos constitucional o inconstitucional. Pues si el legislador, al expedir la ley, se limita a enunciar el asunto a tratar, pero delega en el Presidente todos los temas inherentes a la propia labor legislativa, resulta innegable que estaría trasladando el legislativo su propia facultad constitucional. Al contrario, si la ley establece los parámetros generales, la reglamentación que el Ejecutivo expida es simplemente el resultado de las atribuciones constitucionales propias para desarrollarla.”¹²

En consecuencia, el artículo 5 solo hace enunciaciones simples que derivan que el Presidente asumiría una función legislativa. Así las cosas, las atribuciones previstas en el artículo 5 permiten inferir que el Congreso no está legislando sobre la IA, sino permitirían que el Gobierno Nacional legisle por vía reglamentaria en materias que deberían ser objeto de reserva de ley. Esta situación resulta particularmente problemática en un campo altamente técnico y que requiere control democrático previo. Asimismo, la redacción actual genera incertidumbre regulatoria, ya que el alcance del régimen podría variar según criterios administrativos cambiantes, lo cual es incompatible con la exigencia constitucional de legalidad y reserva de ley.

Lo anterior, reproduce algunas de las dificultades advertidas en la experiencia europea, donde la coexistencia de normas incompletas y reglamentos aun en construcción genera un entorno donde las empresas deben invertir recursos en prepararse para obligaciones de que no conocen con certeza, sin garantías de que las medidas adoptadas sean suficientes o adecuadas al estándar final.¹³

Por otra parte, el listado para la identificación de sistemas críticos contiene imprecisiones técnicas relevantes. En particular, considerar como críticos los “*sistemas diseñados para influir de manera subliminal en el comportamiento humano*” es inadecuado y podría abarcar prácticas legítimas como técnicas de publicidad, videojuegos, interfaces conversacionales o sistemas de

¹² Corte Constitucional. Sentencia C-512 de 1997. M.P. Jorge Arango Mejía.

¹³ Adam Satariano, “EU delays AI law as Big Tech pushes back”, *Financial Times*, 19 de noviembre de 2025, disponible en: <https://www.ft.com/content/6585fb32-8a86-4ffb-a940-06b17e06345a>

recomendación, todos los cuales influyen, en alguna medida, sobre el comportamiento humano. En consecuencia, la legislación debería evitar que casos excepcionales terminen convirtiéndose en prohibiciones absolutas con efectos colaterales sobre tecnologías de uso legítimo.

Finalmente, otro vacío crítico del artículo y del Proyecto de Ley en general, es la ausencia de un tratamiento específico para los modelos de IA de propósito general, que hoy en día constituyen la base del ecosistema global de IA. Su exclusión genera incertidumbre jurídica, pues abre la posibilidad de que estos modelos sean clasificados automáticamente como de alto o crítico riesgo, aun cuando su nivel de riesgo depende del uso concreto y no de la mera existencia.

Por ejemplo, un chatbot conversacional puede realizar acciones que, de acuerdo con las definiciones previstas en el Proyecto de Ley, podrían clasificarse en distintas categorías de riesgo dependiendo de la interacción específica del usuario. En consecuencia, un mismo modelo de propósito general podría quedar sometido simultáneamente a distintos regímenes regulatorios, generando ambigüedad regulatoria.

La literatura especializada ha advertido que regular el modelo por sí solo crea un punto ciego regulatorio. Como lo señala Carey (2025), son los sistemas los que materializan el riesgo. Por lo tanto, la regulación debe enfocarse en el uso concreto del sistema y no penalizar la mera existencia del modelo, puesto esto solo institucionaliza la incertidumbre sin prevenir eficazmente los daños dentro de la cadena de valor¹⁴.

En ese sentido, la regulación debería aclarar que: (i) los modelos de propósito general son , por defecto, de riesgo mínimo o nulo, (ii) las obligaciones surgen únicamente cuando el proveedor controla funcionalidades destinadas a usos de alto riesgo y no por la simple potencialidad del modelo; y (iii) la responsabilidad no recae sobre el desarrollador cuando el implementador utiliza el modelo para fines no previstos, en contextos de riesgo crítico o en actividades expresamente prohibidas.

2.5. Comentarios respecto al artículo 6 “Evaluación de potencial de impacto de sistemas de IA de alto riesgo”

El artículo propuesto exige que el implementador evalúe la calidad y representatividad de los datos, el desempeño del sistema y la mitigación de riesgos, pero omite un aspecto indispensable para garantizar que dicha responsabilidad sea viable. En particular, los proveedores de modelos base o sistemas previamente entrenados deben suministrar la documentación técnica mínima necesaria para que los implementadores puedan cumplir adecuadamente con la evaluación de

¹⁴ Aurora Woods y Thomas King, “Regulating Uncertainty: Governing General-Purpose AI Models and Systemic Risk,” *European Journal of Risk Regulation* (2025), disponible en: resolve.cambridge.org/core/journals/european-journal-of-risk-regulation/article/7EEFE1D8421A43A98CE91F7C697DE538

impacto, especialmente aquella relacionada con la calidad de los datos utilizados durante el entrenamiento del modelo y con los indicadores de desempeño del sistema.

En la práctica, el implementador no siempre tiene acceso al código fuente, a las arquitecturas internas, a los datasets originales ni a la trazabilidad del proceso de entrenamiento. En consecuencia, el artículo traslada al implementador una carga respecto de aspectos sobre los cuales no tiene control, creando un régimen de responsabilidad asimétrico y generando riesgos jurídicos difíciles de gestionar.

En ese sentido, los proveedores de IA que suministren modelos base con potencial de uso de alto riesgo deberían facilitar documentación técnica, en la medida en que ello sea técnicamente posible y sin revelar secretos industriales o información protegida por propiedad intelectual, permitiendo así que el implementador realice una evaluación contextual y proporcional. De lo contrario, la disposición podría convertirse en un mandato sin aplicabilidad real.

Adicionalmente, la obligación de actualizar la evaluación de impacto al menos una vez al año desconoce la naturaleza operativa de los sistemas de IA y las capacidades reales del mercado colombiano. Para muchas organizaciones, especialmente Pymes, instituciones públicas de baja madurez digital y entidades que adoptan IA como servicio, esta exigencia implica costos recurrentes elevados y procesos de auditoría complejos que pueden desincentivar la adopción formal de IA.

En consecuencia, un régimen de evaluación periódico debería estructurarse con base en cambios relevantes en el sistema, eventos de riesgo o evolución de las condiciones de uso, y no a partir de un plazo fijo arbitrario que introduce cargas administrativas desproporcionadas.

2.6. Comentarios respecto al artículo 7 al 14 “Gobernanza para la inteligencia artificial”

Los artículos 7 al 14 del Proyecto de Ley evidencian un diseño institucional completo que delega facultades amplias y abiertas al Ejecutivo, generando inseguridad jurídica. De acuerdo con el Proyecto de Ley, el Ministerio de Ciencia, Tecnología e Innovación actuaría como autoridad nacional en IA y simultáneamente, coordinaría y presidiría el Comité Intersectorial de Coordinación para la IA, instancia integrada por al menos diez entidades públicas y representantes del sector académico, productivo y de la sociedad civil.

Adicionalmente, el artículo 8 autoriza la creación de mesas técnicas, comités especializados y otras instancias adicionales sin establecer criterios claros para su confirmación ni límites funcionales precisos. Estas estructuras se suman a la autoridad nacional, a las instancias creadas para los sandbox regulatorios y a órganos con funciones similares, aumentando la fragmentación institucional, el traslape de competencias y dificultando una gobernanza efectiva.

En ese contexto, resulta necesario simplificar la arquitectura institucional prevista en los artículos 7 al 14, concentrando funciones en una única entidad competente y evitando la proliferación de

órganos consultivos que duplican esfuerzos, afectando los procesos de toma de decisiones y aumentando los costos regulatorios sin aportar valor claro. Una estructura institucional más acotada y con competencias claramente definidas permitiría cumplir los objetivos de gobernanza de la IA sin reproducir una multiplicidad de reguladores que, en otros contextos, ha resultado problemática.

2.7. Comentarios respecto al artículo 18 “Protección de la propiedad industrial en inteligencia artificial y uso legítimo de contenidos”

En primer lugar, el artículo no incorpora una disposición explícita sobre la minería de texto y datos (TDM), práctica indispensable para el entrenamiento de modelos de IA y ampliamente reconocida globalmente como un uso legítimo cuando se realiza contenidos lícitos y accesibles al público.

La ausencia de esta regla genera incertidumbre respecto de si actividades rutinarias de entrenamiento constituyen infracciones a derechos de autor, afectando proyectos de investigación y limitando el desarrollo de modelos. En consecuencia, resulta necesario incluir una cláusula que reconozca la TDM para fines de investigación, desarrollo e innovación, permitiendo su uso salvo que el titular excluya expresamente dicho contenido mediante mecanismos técnicos estandarizados y fácilmente implementables. Una formulación de esta naturaleza no solo garantiza la protección de derechos sino que establece una ruta segura para la innovación.

Asimismo, el artículo exige autorización previa para el uso de voces e imágenes, pero no diferencia entre el simple uso de datos para entrenamiento y la generación de contenidos sintéticos que identifican o imitar a una persona. Esta omisión podría interpretarse erróneamente como una prohibición general a entrenar modelos utilizando datos públicamente disponibles, afectando significativamente la construcción de sistemas de IA en Colombia y convertiría en infractores a desarrolladores legítimos.

En ese sentido, resulta fundamental aclarar que la autorización opera únicamente cuando exista una explotación comercial de la entidad o riesgo real de confusión respecto de la participación de una persona, y no cuando los datos sean utilizados exclusivamente como insumo estadístico para entrenamiento de modelos, sin perjuicio de la aplicación de las normas sobre protección de datos personales.

2.8. Comentarios respecto al artículo 30 “Infracciones administrativas en inteligencia artificial”

El artículo 30 establece las infracciones administrativas aplicables a los responsables de IA. Sin embargo, resulta preocupante que la disposición señale que “serán infracciones, entre otras”, dejando abierta la posibilidad de que el operador jurídico configure infracciones adicionales a las enunciadas taxativamente en el artículo.

Esta formulación genera un riesgo importante de inconstitucionalidad por posible vulneración del principio de legalidad propio del derecho administrativo sancionador. En efecto, el principio de legalidad constituye una garantía esencial del debido proceso consagrado en el artículo 29 de la Constitución Política. Al respecto, la Corte Constitucional ha señalado que:

“En sostenida jurisprudencia la Corte ha hecho ver que la prohibición de imponer sanciones, si no es conforme a normas sustanciales previas que las determinen, resulta extensiva a todos los procedimientos administrativos en los que se pretenda dicha imposición. Al respecto, Corporación ha señalado que en el derecho administrativo sancionador son aplicables mutatis mutandi las garantías superiores que rigen en materia penal, entre ellas la de legalidad de las infracciones y de las sanciones, conforme a la cual nadie puede ser sancionado administrativamente sino conforme a normas preexistentes que tipifiquen la contravención administrativa y señalen la sanción correspondiente. (...)

La finalidad del principio de legalidad de las sanciones, que justifica su adopción constitucional, consiste en garantizar la libertad de los administrados y controlar la arbitrariedad judicial y administrativa mediante el señalamiento legal previo de las penas aplicables. Y aunque la doctrina y la jurisprudencia han reconocido que en el derecho administrativo sancionador, y dentro de él el disciplinario, los principios de tipicidad y legalidad no tienen la misma rigurosidad exigible en materia penal, aun así el comportamiento sancionable debe estar precisado inequívocamente, como también la sanción correspondiente, a fin de garantizar el derecho al debido proceso a que alude el artículo 29 superior.”¹⁵

En este contexto, la amplitud e indeterminación con la que el artículo define las infracciones administrativas introduce escenarios de inseguridad jurídica, en la medida en que permitiría la configuración de conductas sancionables no previstas expresamente por la ley. Esta situación podría vulnerar el principio de legalidad propio del derecho administrativo sancionador, el cual exige la tipificación previa y clara de las conductas y sanciones a imponer con el fin de garantizar el debido proceso consagrado constitucionalmente.

La jurisprudencia ha sido enfática en señalar que la seguridad jurídica y la protección frente a posibles arbitrariedades dependen de que las infracciones estén delimitadas sin ambigüedad. Por lo tanto, resulta necesario ajustar la disposición para evitar riesgos de inconstitucionalidad y asegurar que el régimen sancionatorio en materia de inteligencia artificial se mantenga dentro de los parámetros constitucionales.

2.9. Comentarios respecto al artículo 32 “Medidas correctivas y sanciones”

En primer lugar, la referencia a “autoridades competentes” resulta indeterminada, especialmente si se tiene en cuenta la multiplicidad de autoridades públicas previstos en el Proyecto de Ley como parte de la gobernanza de la IA. Esta amplitud puede generar conflictos de competencia e

¹⁵ Corte Constitucional. Sentencia C-475 de 2004. M.P. Marco Gerardo Monroy Cabra.

incluso riesgos de doble juzgamiento respecto de los mismos hechos, vulnerando el artículo 29 de la Constitución Política.

Asimismo, esta indefinición genera inseguridad jurídica para el ecosistema de IA en Colombia, en la medida en que un mismo desarrollo o despliegue podría ser simultáneamente supervisado y sancionado por diferentes autoridades.

Por otra parte, la posibilidad de imponer medidas como el cierre temporal o definitivo de la operación del sistema de IA, incluyendo el bloqueo de acceso en el territorio nacional cuando existan riesgos graves, deliberados o irreversibles, constituye una medida de máxima intensidad que puede generar afectaciones desproporcionadas sobre usuarios y empresas colombianas que dependen de servicios digitales transfronterizos para su productividad, educación y demás actividades.

Igualmente, se estima que estas medidas deberían ser impuestas por autoridades judiciales y no administrativas. Finalmente, dada la imprecisión técnica del proyecto cualquier conducta puede ser considerada con riesgos graves, deliberados o irreversibles, llevando a la imposición de esta sanción de manera desproporcionada.

3. Conclusión y solicitud respetuosa

El Proyecto de Ley 043 de 2025 Senado - 324 de 2025 Cámara no solo resulta inoportuno en su trámite de urgencia, sino que además presenta problemas sustanciales de conveniencia y constitucionalidad.

Asimismo, el proyecto pretende trasladar este esquema regulatorio a un país en el que el ecosistema de IA aún es incipiente, los niveles de inversión continúan siendo reducidos, la adopción empresarial es limitada y la mayoría del tejido empresarial está conformado por PyMEs que no cuentan con las capacidades técnicas, jurídicas ni financieras necesarias para asumir las cargas propuestas.

En consecuencia, respetuosamente solicitamos archivar el Proyecto de Ley y permitir que el país avance, en su lugar, hacia instrumentos graduales, flexibles y proporcionales, tales como lineamientos técnicos, códigos de conducta, mecanismos de autorregulación, estándares técnicos y estrategias de fortalecimiento institucional y de capacidades empresariales.

Por último, destacamos que la regulación de la IA en Colombia debe ser el resultado de un proceso amplio de deliberación, sustentado en evidencia técnica y en una comprensión realista de las necesidades y capacidades del país.

Esperando haber aportado de manera positiva con nuestros aportes, nos ponemos a sus órdenes en caso de tener alguna duda o inquietud sobre los mismos.

Agradeciendo la atención prestada, me suscribo de Usted con sentimientos de consideración y aprecio.

Cordialmente,

A handwritten signature in black ink, appearing to read 'ALBERTO SAMUEL YOHAI', written over a faint, larger version of the same signature.

ALBERTO SAMUEL YOHAI

Presidente

Cámara Colombiana de Informática y Telecomunicaciones – CCIT