Esta intervención presenta una evaluación jurídica preliminar y sustantiva del Proyecto de Ley 043 de 2025 (Senado) – 324 de 2025 (Cámara), que busca establecer un marco regulatorio integral para la inteligencia artificial (IA) en Colombia.

El análisis examina el proyecto a la luz de las obligaciones vinculantes del Estado colombiano en materia de derecho internacional de los derechos humanos (DIDH) y derecho internacional humanitario (DIH), así como de los principios generales de responsabilidad internacional del Estado.

La intervención responde a las preguntas formuladas en la invitación a la audiencia pública, particularmente en relación con:
(i) el límite entre eficacia operativa y derechos fundamentales;
(ii) el significado y alcance de la soberanía tecnológica;
(iii) la responsabilidad por los daños causados por sistemas de IA; y
(iv) las salvaguardas necesarias para garantizar la compatibilidad con el derecho internacional.

Colombia es Estado Parte, entre otros instrumentos, de:

- El Pacto Internacional de Derechos Civiles y Políticos (PIDCP)
- La Convención Americana sobre Derechos Humanos (CADH)
- El Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC)
- La Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW)
- La Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial (ICERD)
- Los cuatro Convenios de Ginebra de 1949 y el Protocolo Adicional II

La regulación de la inteligencia artificial debe basarse en el derecho internacional de los derechos humanos como marco normativo central. Los Estados tienen la obligación de garantizar que el desarrollo, adquisición y despliegue de sistemas de IA respeten los derechos fundamentales y cuenten con salvaguardas jurídicas adecuadas.

En virtud del artículo 2(1) del PIDCP y del artículo 1(1) de la CADH, Colombia debe respetar y garantizar los derechos reconocidos en dichos instrumentos a todas las personas bajo su jurisdicción. Conforme al artículo 2 de la CADH y al artículo 2(2) del PIDCP, debe adoptar las medidas legislativas y de otra índole necesarias para

hacer efectivos tales derechos. Estas obligaciones incluyen deberes positivos de regular, supervisar, investigar y prevenir daños previsibles derivados del despliegue de tecnologías emergentes.

Dado que los sistemas de IA amplifican el poder estatal mediante la escala, la automatización, la capacidad predictiva y la opacidad técnica, su uso en vigilancia, funciones policiales, procesos judiciales, control migratorio, gestión fronteriza y operaciones militares exige un escrutinio jurídico reforzado. La regulación preventiva no es una opción política discrecional, sino una obligación derivada de los tratados internacionales.

1. ***El uso de Inteligencia Artificial en seguridad plantea una tensión estructural entre eficacia operacional y protección de derechos fundamentales. ¿Dónde debe trazarse ese límite en el caso colombiano? ¿existe alguna tecnología de vigilancia y seguridad basada en Inteligencia Artificial que consideran inaceptable bajo cualquier circunstancia, incluso con orden judicial?***

El derecho internacional de los derechos humanos permite determinadas restricciones a derechos como la privacidad, la libertad y la expresión cuando sean estrictamente necesarias para perseguir fines legítimos como la seguridad nacional o el orden público. Sin embargo, toda restricción debe cumplir de manera acumulativa con los principios de legalidad, finalidad legítima, necesidad y proporcionalidad, tal como han sido interpretados de forma constante por el Comité de Derechos Humanos y la Corte Interamericana de Derechos Humanos. Los marcos regulatorios deben evitar excepciones amplias para ámbitos como la seguridad nacional, la aplicación de la ley o la gestión migratoria, ya que estos son precisamente los contextos en los que el uso de sistemas de IA puede generar mayores riesgos para los derechos humanos.

El límite constitucional y convencional a la eficacia operativa se alcanza cuando los sistemas de IA socavan estos principios al permitir injerencias indiscriminadas, eliminar el control humano significativo o impedir la revisión judicial efectiva.

La vigilancia biométrica habilitada por IA, el reconocimiento facial en tiempo real, la policía predictiva y el análisis masivo de datos comprometen directamente:

- El artículo 17 del PIDCP (derecho a la vida privada)
- El artículo 11 de la CADH (protección de la honra, dignidad y vida privada)

La capacidad estructural de los sistemas de IA para permitir monitoreo persistente y agregación masiva de datos puede transformar la vigilancia dirigida en observación generalizada o indiscriminada. A diferencia de los métodos tradicionales de investigación, estas tecnologías pueden operar de forma continua e invisible, afectando poblaciones enteras.

La vigilancia biométrica masiva en espacios públicos —sin sospecha individualizada ni autorización judicial previa— plantea serias dudas de proporcionalidad y puede constituir una injerencia arbitraria contraria a los artículos 17 del PIDCP y 11 de la CADH.

Dado el contexto histórico colombiano, marcado por conflicto armado interno y antecedentes de abusos en materia de inteligencia, el análisis de proporcionalidad debe ser especialmente estricto e incorporar salvaguardas como autorización judicial previa, limitación de finalidad, minimización de datos, límites de conservación y supervisión independiente.

Los sistemas automatizados de evaluación de riesgo y predicción utilizados en funciones policiales, acceso a servicios públicos, administración de justicia, crédito, empleo o migración involucran:

- Los artículos 2(1) y 26 del PIDCP
- Los artículos 1(1) y 24 de la CADH
- La ICERD
- La CEDAW

Los sesgos algorítmicos que afecten de manera desproporcionada a comunidades afrocolombianas, pueblos indígenas, poblaciones rurales, migrantes o mujeres pueden constituir discriminación indirecta en el sentido del derecho internacional, incluso en ausencia de intención discriminatoria. Informes recientes de las Naciones Unidas han advertido que los sistemas de inteligencia artificial utilizados en contextos de seguridad pública, control migratorio y prestación de servicios públicos pueden reproducir o amplificar desigualdades estructurales presentes en los datos utilizados para su entrenamiento, lo que exige evaluaciones rigurosas de impacto en igualdad y mecanismos continuos de supervisión.

En virtud de la ICERD y la CEDAW, Colombia tiene obligaciones reforzadas de debida diligencia para prevenir tanto la discriminación directa como la indirecta. Esto exige evaluaciones de impacto en igualdad, pruebas de sesgo, uso de datos representativos y monitoreo continuo de sistemas de alto riesgo. Los riesgos de discriminación no se originan únicamente en los algoritmos, sino también en las prácticas de recopilación y tratamiento de datos que alimentan dichos sistemas.

La falta de prevención de impactos discriminatorios previsibles puede constituir por sí misma una violación de la obligación de garantizar la igualdad ante la ley.

Los sistemas de IA que influyen en decisiones de detención, recomendaciones de sentencia, determinaciones migratorias, clasificación de riesgo o valoración probatoria comprometen:

- El artículo 9 del PIDCP (libertad y seguridad personal)
- El artículo 14 del PIDCP (garantías de debido proceso)
- Los artículos 7 y 8 de la CADH (libertad personal y garantías judiciales)

La opacidad algorítmica puede afectar el derecho de defensa, el principio de contradicción, la igualdad de armas y la obligación de motivar las decisiones.

El secreto comercial no puede prevalecer sobre el derecho a una defensa efectiva cuando herramientas automatizadas inciden en la libertad o en otros derechos fundamentales. El control humano significativo y el derecho a una explicación suficiente son condiciones necesarias para el cumplimiento convencional.

Los sistemas de uso de la fuerza asistidos por IA, incluidas las armas autónomas y las herramientas de selección de objetivos, comprometen directamente:

- El artículo 6 del PIDCP (derecho a la vida)
- El artículo 4 de la CADH (derecho a la vida)

En situaciones de conflicto armado, el DIH se aplica de manera concurrente con el DIDH. El marco jurídico aplicable incluye:

- El artículo común 3 de los Convenios de Ginebra
- El Protocolo Adicional II
- Los principios consuetudinarios de distinción, proporcionalidad, precaución y necesidad militar

Los sistemas que carecen de control humano significativo plantean serias dudas sobre el cumplimiento de los principios de distinción y proporcionalidad, especialmente en entornos complejos con presencia de población civil.

Conforme al artículo 36 del Protocolo Adicional I —ampliamente reconocido como reflejo del derecho consuetudinario— los Estados deben realizar revisiones jurídicas de nuevas armas, medios o métodos de guerra antes de su adquisición o despliegue. Los sistemas de IA con capacidad letal o que incidan en la selección de objetivos están comprendidos en esta obligación.

En consecuencia, todo sistema militar o de seguridad basado en IA que pueda afectar la vida debe someterse a una revisión jurídica rigurosa ex ante para garantizar su compatibilidad con el DIH y con el carácter no derogable del derecho a la vida.

2. ***Colombia depende mayoritariamente de proveedores extranjeros para sus sistemas de Inteligencia Artificial en seguridad. ¿Qué disposiciones debería incluir el proyecto de ley 043 de 2025 Senado – 324 de 2025 Cámara para garantizar soberanía tecnológica, y cuál sería el equilibrio adecuado entre adquisición de tecnología extranjera y desarrollo de capacidades nacionales?***

La soberanía tecnológica no debe entenderse como aislamiento de los mercados tecnológicos globales, sino como la capacidad del Estado para ejercer control regulatorio efectivo sobre las tecnologías que despliega.

Conforme al derecho internacional de la responsabilidad del Estado, Colombia sigue siendo internacionalmente responsable por violaciones atribuibles a sus autoridades, incluidos los daños causados por sistemas de IA utilizados en funciones públicas, independientemente de si fueron desarrollados internamente o adquiridos a proveedores extranjeros.

La externalización tecnológica no transfiere la responsabilidad jurídica internacional.

Cuando el secreto propietario impide la auditabilidad o la explicabilidad, las personas afectadas pueden verse privadas de:

- El artículo 2(3) del PIDCP (derecho a un recurso efectivo)

- El artículo 25 de la CADH (protección judicial)

Los marcos de contratación pública deben, por tanto, exigir transparencia, acceso a auditorías, explicabilidad, supervisión humana y certificación de cumplimiento para sistemas de alto riesgo.

3. ***Si un sistema de reconocimiento facial identifica erróneamente a una persona, o un sistema autónomo toma una decisión letal equivocada en el marco del conflicto armado: ¿quién respondería penalmente, civil y disciplinariamente? ¿El marco de responsabilidad del proyecto de ley 043 de 2025 Senado – 324 de 2025 Cámara suficiente para estos escenarios?***

Cuando sistemas de inteligencia artificial son desplegados por autoridades públicas, los actos resultantes son atribuibles al Estado en el plano del derecho internacional. De acuerdo con los Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (ARSIWA), los actos realizados mediante sistemas automatizados son atribuibles al Estado cuando son ejecutados por sus órganos o bajo su autoridad. El Estado responde por daños que afecten derechos fundamentales como la vida, la libertad, la igualdad y el debido proceso, así como por la obligación de garantizar reparación integral. Paralelamente, los individuos pueden asumir **responsabilidad penal** (por ejemplo, comandantes bajo responsabilidad de mando u operadores negligentes), **civil** (Estado, proveedores o funcionarios) y **disciplinaria (**por omisión de supervisión o control adecuados), asegurando que exista rendición de cuentas efectiva ante errores o daños causados por la IA.

Una rendición de cuentas efectiva requiere:

1. Atribución clara de responsabilidad
2. Trazabilidad y documentación de decisiones automatizadas
3. Derecho a explicación suficiente para revisión judicial
4. Acceso a órganos de supervisión independientes y tribunales
5. Mecanismos de reparación, incluida restitución e indemnización

Sin estas salvaguardas, las víctimas de identificación errónea, detención indebida, discriminación o uso ilícito de la fuerza pueden verse privadas de un recurso

efectivo en violación de las obligaciones convencionales.

4. ***¿Qué acciones cree debe desarrollar el Estado colombiano en materia de regulación o protección de los derechos humanos frente a sistemas de Inteligencia Artificial?***

La gobernanza de la IA involucra la rendición de cuentas democrática. La transparencia constituye una salvaguarda estructural necesaria para garantizar la legalidad y previsibilidad exigidas por el derecho internacional de los derechos humanos.

El Proyecto de Ley debería:

- Fortalecer el control parlamentario sobre el uso de IA de alto riesgo
- Exigir informes públicos periódicos (sujetos a limitaciones legítimas y proporcionales de seguridad nacional)
- Garantizar protección a denunciantes
- Facilitar la participación de la sociedad civil
- Establecer autoridades de supervisión independientes con competencias efectivas de investigación, auditoría y sanción para supervisar el uso de sistemas de IA de alto riesgo.

Estos mecanismos refuerzan el orden constitucional y la legitimidad democrática.

En virtud del artículo 2 de la CADH y del artículo 2(2) del PIDCP, Colombia debe adoptar medidas preventivas cuando los riesgos sean previsibles. La expansión acelerada de sistemas de IA hace que dichos riesgos sean claramente previsibles.

A nivel internacional, la Office of the United Nations High Commissioner for Human Rights ha precisado el alcance de estas obligaciones preventivas en el contexto de la inteligencia artificial. En su informe *“El derecho a la privacidad en la era digital”* (A/HRC/51/17, 2022), la Alta Comisionada señaló que los Estados deben realizar evaluaciones de impacto en derechos humanos antes del despliegue de sistemas de IA de alto riesgo y advirtió que determinadas aplicaciones —en particular la vigilancia biométrica en tiempo real en espacios públicos— pueden resultar incompatibles con el derecho internacional de los derechos humanos si no cumplen estrictamente los principios de legalidad, necesidad y proporcionalidad. Asimismo, los United Nations Guiding Principles on Business and Human Rights refuerzan el deber estatal de regular y supervisar a proveedores privados de tecnología

mediante marcos normativos adecuados, exigencias de debida diligencia y garantías efectivas de acceso a recursos cuando se produzcan afectaciones.

La regulación preventiva incluye:

- Evaluaciones obligatorias de impacto en derechos humanos
- Monitoreo en materia de igualdad y no discriminación
- Auditorías independientes de sesgo
- Revisión continua de cumplimiento
- Preservación de control humano significativo en decisiones coercitivas
- Revisiones jurídicas conforme al artículo 36 del DIH para aplicaciones militares

Estas medidas concretan las obligaciones positivas del Estado en el marco del derecho internacional.