



SENADO DE LA REPÚBLICA
SECRETARÍA GENERAL LEGISLATIVA
9/6/2025 - 3:42 PM
FECHA HORA
RECIBIDO POR Rosaura Sandoz
SIL-00818

SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

LEY DE USO ÉTICO Y SEGURO DE LA INTELIGENCIA ARTIFICIAL DE LA REPÚBLICA DOMINICANA

Considerando primero: Que la inteligencia artificial (IA) ofrece beneficios económicos y sociales en múltiples sectores, pero también plantea riesgos para la privacidad, la seguridad y los derechos fundamentales, se hace necesario un marco jurídico que promueva su uso responsable, ético y seguro. Este proyecto de ley se alinea con la Ley de IA de la Unión Europea (Reglamento UE 2024/1689), adaptando a nuestra realidad los principios de derecho internacional y comparado (Canadá, EE.UU., Japón, Singapur) y garantizando la conformidad con la Constitución y leyes vigentes de la República Dominicana;

Considerando segundo: Que la IA ya no es una tecnología del futuro, sino una herramienta del presente con impacto directo en la salud, la educación, la justicia, la economía, la ciberseguridad y la gestión pública. Su regulación no solo es necesaria, sino urgente;

Considerando tercero: Que es necesario Proteger los derechos fundamentales de las personas ante sistemas automatizados así como fomentar el desarrollo tecnológico, la innovación y el uso ético de la inteligencia artificial;

Considerando cuarto: Que se hace necesario establecer un marco claro de responsabilidades, supervisión, transparencia y seguridad en el uso de IA y crear instituciones especializadas como la Autoridad Nacional de Inteligencia Artificial (ANIA), y promover el talento humano y la inclusión digital;

Considerando quinto: Que es un imperativo la regulación de los sistemas de Inteligencia Artificial (AI) por lo que resulta necesario un régimen de regulación específica que garantice el respeto a los derechos fundamentales, la igualdad, la privacidad y la seguridad de las personas frente a los riesgos y desafíos que plantea su uso;

Considerando sexto: Que la Constitución de la República Dominicana en su artículo 8 establece lo siguiente: *"Es función esencial del Estado, la protección efectiva de los derechos de la persona, el respeto a su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatible con el orden público y el bienestar general y el derecho de todos y todas"*.

Vista: La Constitución de la República Dominicana;

Vista: La Ley núm. 139-01, del 13 de agosto de 2001, Ley que crea el Sistema Nacional de Educación Superior Ciencia y Tecnología;

Vista: La Ley núm. 200-04, del 28 de julio de 2004, Ley General sobre Libre Acceso a la Información Pública y Reglamento de Aplicación;

Vista: La Ley núm. 53-07, del 23 de abril de 2007, Ley sobre crímenes y delitos de alta tecnología;

Vista: La Ley núm. 172-13, del 13 de diciembre de 2013, sobre protección de datos personales;

Visto: El Decreto 230-18, del 15 de junio de 2018, que establece y regula la estrategia nacional de ciberseguridad;

Visto: El Reglamento del Senado de la República.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

HA DADO LA SIGUIENTE LEY:

CAPITULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto. Esta ley tiene por objeto establecer un marco jurídico integral para el desarrollo, la puesta en servicio, uso y supervisión de sistemas de Inteligencia Artificial (IA) en la República Dominicana, aplicable a todos los sectores económicos y sociales. Se busca promover el uso responsable, ético y seguro de la IA, impulsando la innovación tecnológica sin imponer restricciones innecesarias, a la vez que se protegen la dignidad humana, la autonomía personal, la igualdad y los derechos fundamentales consagrados en la Constitución. La presente ley garantiza además la seguridad jurídica para los innovadores y usuarios de IA, fomentando la confianza pública en estas tecnologías.

Artículo 2. Ámbito de aplicación. Las disposiciones de esta ley se aplican a todas las personas físicas y jurídicas, instituciones públicas y privadas, nacionales o extranjeras, que desarrollen, implementen, distribuyan o utilicen sistemas de IA en el territorio de la República Dominicana. Quedan incluidos los sistemas de IA integrados en productos o servicios ofrecidos en el país. Se excluyen del ámbito de esta ley únicamente los sistemas de IA desarrollados o utilizados con fines militares, de defensa o de seguridad nacional, los cuales estarán sujetos a regulaciones especiales independientes. En ningún caso las exclusiones podrán interpretarse en detrimento de los derechos humanos y principios democráticos fundamentales.

Artículo 3. Definiciones. A los fines de esta ley, se establecen las definiciones siguientes:

- **Inteligencia Artificial (IA):** Sistema basado en tecnología de la información, diseñado para funcionar con cierto grado de autonomía y capaz de, para objetivos explícitos o implícitos, inferir patrones a partir de datos de entrada y generar resultados de salida (predicciones, recomendaciones, decisiones, contenido u otros) que pueden influir en entornos físicos o virtuales. Incluye métodos de aprendizaje automático, lógica simbólica u otras técnicas analíticas para simular capacidades cognitivas humanas.

- **Sistema de IA de Uso General:** Modelo o sistema de IA entrenado para ser adaptable a una amplia variedad de tareas generales, que puede ser integrado en otros sistemas o utilizado en múltiples dominios. Por su naturaleza polivalente, estos modelos fundamentales pueden entrañar riesgos sistémicos cuando poseen capacidades de gran impacto o son utilizados masivamente.

- **Proveedor:** Persona física o jurídica (incluyendo autoridades públicas u organismos) que desarrolla un sistema de IA, o que lo introduce en el mercado o pone en servicio bajo su nombre o marca, ya sea a título oneroso o gratuito.

- **Responsable del despliegue (Operador):** Persona física o jurídica (incluyendo autoridades públicas) que utiliza un sistema de IA bajo su autoridad directa en un contexto concreto (salvo uso personal y no profesional). Equivale al usuario implementador que decide aplicar una IA para un fin determinado y se responsabiliza de su funcionamiento.

- **Datos personales:** Cualquier información sobre una persona física identificada o identificable, según definida por la Ley No. 172-13 sobre Protección de Datos Personales. Incluye datos biométricos (datos derivados de mediciones biológicas únicas



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

como rasgos faciales, huellas dactilares, iris, voz, etc.) utilizados para identificar o categorizar personas.

•**Riesgo (en IA):** La combinación de la probabilidad de que un sistema de IA cause un perjuicio y la gravedad de dicho perjuicio sobre la seguridad, la salud, los derechos fundamentales u otros intereses legítimos de personas o colectivos. Los niveles de riesgo de los sistemas de IA (inadmisible, alto, limitado o mínimo) se definen en esta ley para establecer medidas proporcionales.

Artículo 4. Principios. La aplicación de esta ley se guiará por los siguientes principios éticos y jurídicos fundamentales:

1. Respeto a los Derechos Humanos y la Dignidad: Todo desarrollo o uso de IA debe respetar la dignidad intrínseca de las personas, sus derechos fundamentales y valores democráticos. Se prohíbe la discriminación injusta por motivo de género, raza, origen étnico, orientación sexual, opinión política, estado de salud u otra condición, y se fomentará la inclusión de grupos vulnerables en la sociedad digital.

2. Enfoque Centrado en el Ser Humano: La IA ha de estar al servicio de las personas; su diseño, implementación y uso debe reforzar el bienestar humano, la igualdad y la libertad, sin menoscabar la autonomía personal ni sustituir indebidamente la toma de decisiones humanas en ámbitos donde los valores éticos o el juicio humano sean indispensables. Las personas tienen derecho a intervenir y a obtener explicaciones en decisiones automatizadas que les afecten significativamente.

3. Transparencia y Explicabilidad: Los sistemas de IA deberán ser transparentes en su funcionamiento, proporcionando información clara, accesible y comprensible sobre cómo llegan a sus conclusiones y los criterios que utilizan. Sus algoritmos y procesos decisionales deberán ser auditables en la medida de lo posible, lo que permitirá generar confianza, facilitar la detección y corrección de sesgos o errores, y garantizar la rendición de cuentas.

4. Responsabilidad y Rendición de Cuentas: Los desarrolladores, proveedores y usuarios de sistemas de IA serán responsables por el funcionamiento de estos y por los efectos que produzcan. Deben rendir cuentas ante las autoridades y el público, especialmente cuando la IA tome decisiones con impacto legal o significativo sobre individuos. La utilización de IA no exime a las personas ni a las entidades de sus obligaciones legales preexistentes ni de responsabilidad por daño que pudieran causar.

5. Privacidad y Protección de Datos: El tratamiento de datos personales en sistemas de IA debe realizarse conforme a la legislación de protección de datos vigente, garantizando en todo momento la privacidad, confidencialidad e integridad de los datos personales. Se promoverá la aplicación de técnicas de mejora de la privacidad (anonimización, seudonimización, encriptación) en el entrenamiento y operación de modelos de IA. Cualquier sistema de IA que procese información personal o utilice contenido audiovisual relativo a personas deberá garantizar la privacidad, la protección de datos, la integridad personal y demás derechos fundamentales de los ciudadanos involucrados.

6. Seguridad, Robustez y Ciberseguridad: Los sistemas de IA deben ser diseñados y desarrollados de forma segura y robusta, evitando comportamientos impredecibles. Se deberán tomar medidas de ciberseguridad adecuadas para proteger los sistemas de IA contra accesos no autorizados, manipulaciones maliciosas, filtración de datos o ataques que puedan comprometer su funcionamiento o los datos que manejan. La IA debe



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

incorporar mecanismos de seguridad por diseño y resistencia a fallos, especialmente en aplicaciones críticas.

7. Justicia Algorítmica y No Discriminación: Es imperativo identificar y mitigar posibles sesgos en los datos o algoritmos que pudieran resultar en tratamientos discriminatorios. Los sistemas de IA deben someterse a evaluaciones periódicas para detectar sesgos raciales, de género u otros, corrigiendo de inmediato cualquier disparidad injustificada en sus resultados. Se promoverá un desarrollo inclusivo de la IA considerando la diversidad de usuarios; por ejemplo, fomentando equipos de desarrollo diversos y conjuntos de datos representativos para evitar visiones parciales o excluyentes.

8. Supervisión Humana y Control: La IA debe contar con mecanismos de control humano apropiados. En particular, en sistemas de alto riesgo (definidos más adelante), se garantizará que personas competentes supervisen su funcionamiento y puedan intervenir, modificar o desactivar el sistema cuando sea necesario para prevenir un daño. Ningún sistema de IA debe tener la potestad de adopción de decisiones irreversibles o ejecutorias sin intervención humana en ámbitos que afecten derechos fundamentales (ej. denegar un beneficio público sin revisión humana).

9. Transparencia Pública y Participación: Se fomentará la publicación de información sobre el uso de IA en el sector público, de modo que los ciudadanos conozcan qué sistemas se utilizan para la prestación de servicios públicos o la toma de decisiones administrativas que les conciernan. Asimismo, las políticas nacionales en materia de IA deberán formularse promoviendo la participación de expertos, sector privado, academia y sociedad civil (gobernanza colaborativa), conforme a los mandatos de la UNESCO y otras organizaciones internacionales.

10. Innovación Responsable y Proporcionalidad Regulatoria: Las medidas reguladoras establecidas en esta ley se aplicarán conforme al nivel de riesgo de los sistemas de IA, de forma proporcional: los sistemas de mayor riesgo tendrán obligaciones más estrictas, mientras que las de bajo riesgo estarán sujetas a requisitos mínimos o meras recomendaciones. Este enfoque escalonado busca evitar cargas innecesarias a la innovación y a las pequeñas empresas, a la vez que garantiza la seguridad y la confianza. Se promoverá activamente la investigación científica, el desarrollo tecnológico y la inversión en IA, incluyendo incentivos y entornos de prueba controlados (sandboxes regulatorios) para soluciones innovadoras.

CAPÍTULO II

CLASIFICACIÓN Y REGULACIÓN DE LOS SISTEMAS DE IA SEGÚN EL RIESGO

Artículo 5. Categorías de Riesgo. Los sistemas de IA se clasifican en las siguientes categorías, en atención al nivel de riesgo que puedan entrañar para la seguridad, la salud, los derechos fundamentales o intereses legítimos de las personas y la sociedad:

1. Sistemas de Riesgo Inadmisible (Prácticas Prohibidas): Son aquellos sistemas o aplicaciones de IA cuyas características o usos se consideran contrarios a los valores fundamentales, los derechos humanos o la seguridad pública. Estos sistemas se prohíben absolutamente en el territorio nacional por implicar un riesgo intolerable. Se incluyen, entre otros:



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

- a) Sistemas de "score" o clasificación social que evalúen o califiquen la confiabilidad, características o méritos personales de individuos en base a su comportamiento, estatus socioeconómico, preferencias o cualquier dato personal, con el propósito de limitar sus derechos u oportunidades (ya sea por entidades públicas o privadas).
- b) Sistemas que utilicen técnicas subliminales o manipulativas más allá de la percepción consciente, dirigidas a personas o grupos específicos, con el fin de influir en su comportamiento de manera que les pueda causar un perjuicio físico, psicológico, patrimonial o de otra índole. (Por ejemplo, IA incorporada en aplicaciones que manipulen emocionalmente a usuarios vulnerables para inducir acciones perjudiciales).
- c) Sistemas de IA que exploten vulnerabilidades de grupos vulnerables, tales como niños, personas con discapacidades o poblaciones en extrema vulnerabilidad, para distorsionar significativamente su comportamiento de forma que puedan resultar lesionados sus derechos o bienestar.
- d) Sistemas de identificación biométrica remota en tiempo real en espacios públicos con fines de seguridad o control poblacional, salvo las excepciones estrictamente previstas en esta ley. Queda prohibido el uso de sistemas que, mediante cámaras u otros sensores, identifiquen a personas en tiempo real en lugares públicos, ya sea con fines de vigilancia masiva, policiales o de otro tipo, por considerar que afectan desproporcionadamente el derecho a la privacidad, la libertad de tránsito y otros derechos fundamentales. (Excepcionalmente, podrá autorizarse su uso posterior (no en tiempo real) por las fuerzas de seguridad del Estado para la investigación de delitos graves o búsqueda de personas desaparecidas, mediando orden judicial motivada y observando las garantías legales. En ningún caso se usará para vigilancia generalizada).
- e) Sistemas de categorización biométrica que clasifiquen a las personas según características sensibles derivadas de sus rasgos físicos o conductuales (por ejemplo, origen étnico, género, orientación sexual, convicciones políticas o religiosas) a partir de datos biométricos. Se prohíbe su uso para etiquetar o segregar personas en base a categorías protegidas, dado el alto riesgo de discriminación y violación de la dignidad humana.
- f) Sistemas de IA para reconocimiento o inferencia de emociones en entornos como el empleo, la educación o los servicios públicos, utilizados para evaluar, clasificar o influir en personas. Se prohíbe en particular cualquier sistema que intente determinar estados emocionales internos de los individuos (ej. nivel de estrés, honestidad, estado mental) para tomar decisiones en el ámbito laboral, educativo, policial o similar, ya que carecen de suficiente base científica y pueden vulnerar la privacidad y la igualdad. (No se prohíben las aplicaciones de detección emocional con fines médicos o terapéuticos consentidos, ni las de uso personal recreativo, siempre que no produzcan efectos jurídicos adversos sobre terceros).
- g) Uso de sistemas de IA con fines militares, armamentísticos o de guerra electrónica que puedan poner en riesgo la vida humana o la paz pública. En concordancia con el ámbito de aplicación de esta ley, se prohíbe el desarrollo, importación o despliegue de armas autónomas letales u otros sistemas de IA destinados a fines militares, de defensa o seguridad del Estado, en tanto su utilización podría contravenir principios humanitarios y constitucionales.
- h) Cualquier otro uso de IA expresamente prohibido por tratados internacionales de los que la República Dominicana sea parte o por normativa interna especial. (La Autoridad competente podrá actualizar, mediante disposiciones complementarias, la lista de



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

prácticas prohibidas en función de la evolución tecnológica y las recomendaciones internacionales, garantizando siempre su coherencia con principios constitucionales.)

2. Sistemas de IA de Alto Riesgo: Son aquellos sistemas de IA cuyo uso previsto puede tener un impacto significativo adverso en la seguridad, la salud o los derechos fundamentales de las personas, de manera que requieren requisitos y controles estrictos antes y durante su utilización. Esta categoría incluye un número limitado de sistemas definidos por la ley, clasificados en dos subgrupos:

a) Sistemas de IA integrados en productos o servicios sujetos a normativa de seguridad existente: Por ejemplo, componentes de IA que formen parte de infraestructuras críticas (energía, transporte, agua, telecomunicaciones), de dispositivos médicos y sanitarios, vehículos autónomos, equipos de maquinaria industrial, juguetes conectados, o cualquier producto que, para su comercialización, deba cumplir estándares obligatorios de seguridad o requerir certificaciones previas. Si un componente de IA puede influir en el funcionamiento seguro de tales productos (p. ej. un algoritmo de conducción autónoma en un vehículo), dicho sistema de IA se considerará de alto riesgo y deberá cumplir tanto con las regulaciones sectoriales aplicables como con los requisitos de esta ley.

b) Sistemas de IA autónomos utilizados en ámbitos sensibles con posible impacto en derechos fundamentales: Comprende, entre otros:

- Educación y formación profesional: IA utilizada para evaluar estudiantes (por ejemplo, sistemas de calificación de exámenes, admisión a instituciones educativas) o para guiar decisiones en programas formativos, cuya salida pueda influir decisivamente en el futuro educativo o profesional de una persona.

- Empleo, gestión laboral y recursos humanos: IA empleada en procesos de selección de personal, evaluación de desempeño, promoción, asignación de tareas o despido. Estos sistemas pueden afectar el derecho al trabajo y la igualdad de oportunidades, por lo que se les considera de alto riesgo y sujetos a estricta supervisión.

- Acceso a servicios esenciales públicos o privados: Sistemas de IA utilizados para determinar el acceso de personas a servicios o beneficios básicos, tales como préstamos bancarios y calificación crediticia, seguros (por ejemplo, de vida o salud), viviendas en alquiler, programas de asistencia social, subsidios o prestaciones médicas. Decisiones automatizadas en estos ámbitos pueden impactar gravemente las condiciones de vida de las personas (derecho a la salud, vivienda digna, seguridad social, etc.), requiriendo garantías adicionales.

- Aplicaciones en el ámbito de la justicia y los procesos legales: Cualquier sistema de IA utilizado para apoyar o tomar decisiones en actividades propias del Poder Judicial o administrativo sancionador, como herramientas de ayuda a jueces para determinar sentencias o penas, evaluación automatizada de perfiles de riesgo de reincidencia penal, análisis predictivo delictual, o sistemas que realicen perfilamiento de personas con fines de seguridad pública. Aunque la decisión final recaiga en una autoridad humana, el solo aporte de IA en estos procesos exige máxima fiabilidad, transparencia y posibilidad de explicación, dadas las implicaciones en derechos como el debido proceso y la presunción de inocencia.

- Gestión migratoria y fronteriza: Sistemas de IA aplicados en control migratorio, evaluación de solicitudes de visa, asilo o residencia, u otros procesos que determinen



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

el estatus migratorio de individuos. Por implicar posibles riesgos a los derechos de migrantes y el principio de no devolución, se consideran de alto riesgo.

- Aplicaciones de IA en fuerzas del orden y seguridad ciudadana: Por ejemplo, herramientas de análisis predictivo para prevenir delitos, sistemas de evaluación de comportamiento para vigilancia policial, o identificación biométrica a posteriori (no en tiempo real) de sospechosos a partir de bases de datos. Estos sistemas pueden afectar libertades y derechos fundamentales, por lo que su uso estará fuertemente regulado y limitado a supuestos autorizados por la ley. (Se subraya que la identificación biométrica en tiempo real está prohibida salvo excepción judicial per el inciso d) anterior.)

- Cualquier otro sistema de IA que, por disposición del reglamento de esta ley, se considere de alto riesgo debido a su impacto en la seguridad pública, la salud de las personas, el medio ambiente o los derechos fundamentales. La Autoridad Nacional de IA podrá proponer la inclusión de sistemas adicionales a esta categoría, fundamentándolo en evaluaciones de impacto y conforme a estándares internacionales.

Los sistemas de alto riesgo quedan sujetos a una regulación intensiva y al cumplimiento de requisitos obligatorios específicos antes de su puesta en servicio y durante todo su ciclo de vida. Estos requisitos se definen en el Artículo 7 de esta ley e involucran a todos los agentes en la cadena de suministro o uso (proveedores, importadores, distribuidores, responsables de despliegue), de forma tal que ninguno pueda eludir la responsabilidad sobre el sistema.

3.Sistemas de IA de Riesgo Limitado: Son aquellos sistemas de IA que, sin caer en categorías de alto riesgo o prohibidas, pueden suponer ciertos riesgos residuales en materia de posibles manipulaciones, sesgos o confusión de los usuarios. En general, incluyen aplicaciones de IA que interactúan directamente con seres humanos o generan contenido potencialmente engañoso. Si bien su uso es lícito sin necesidad de autorizaciones previas, estarán sujetos a obligaciones de transparencia específicas para mitigar riesgos (conforme al Artículo 8). Ejemplos de sistemas de riesgo limitado: asistentes virtuales conversacionales (chatbots), sistemas generativos de imágenes, audio o video (ej. creadores de contenido "deepfake"), agentes artificiales capaces de hacerse pasar por humanos en comunicaciones, entre otros. Cuando exista peligro claro de confusión o manipulación del usuario –por ejemplo, un chatbot que pueda ser erróneamente percibido como humano, o un contenido multimedia sintético que simule realidad– el proveedor deberá cumplir con las medidas de transparencia señaladas en esta ley. Fuera de dichas obligaciones específicas, estos sistemas podrán desarrollarse y utilizarse con arreglo a la legislación vigente general, adhiriéndose voluntariamente a códigos de conducta recomendados.

4.Sistemas de IA de Riesgo Mínimo o Nulo: Comprende todas las demás aplicaciones de IA no incluidas en las categorías anteriores, cuyo potencial de daño es trivial o inexistente. Ejemplos: filtros de correo no deseado, algoritmos de recomendación de baja sensibilidad, juegos basados en IA, herramientas de ofimática inteligente, etc. Estos sistemas no estarán sujetos a requisitos adicionales obligatorios bajo esta ley, más allá del respeto a la normativa general aplicable (incluida la de protección de datos, ciberseguridad y propiedad intelectual). Se alienta, no obstante, a los desarrolladores y usuarios de estas IA de bajo riesgo a adoptar buenas prácticas voluntarias de ética y seguridad. La Autoridad Nacional podrá emitir lineamientos o directrices no vinculantes para estas aplicaciones a fin de fomentar la calidad, sin que ello suponga cargas regulatorias.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Artículo 6. Artículo 6. Registro Nacional de Sistemas de IA. Con el fin de garantizar la transparencia y el control adecuados, créase el Registro Nacional de Inteligencia Artificial, administrado por la Autoridad creada en esta ley. Se establecen las siguientes disposiciones:

- Registro obligatorio de sistemas de alto riesgo: Todo sistema de IA clasificado como alto riesgo que vaya a ser comercializado, implementado o utilizado en la República Dominicana deberá inscribirse en el Registro antes de su puesta en servicio. La inscripción incluirá, al menos, información detallada sobre: el propósito y ámbito de uso del sistema, sus principales funcionalidades, los algoritmos o técnicas empleados, las categorías de datos utilizados (incluyendo si emplea datos personales o sensibles), las medidas de seguridad y ciberseguridad implementadas, así como la identificación del proveedor, del responsable del despliegue local y, en su caso, del importador o distribuidor.
- Registro de otros sistemas cuando se requiera: La Autoridad Nacional de IA podrá requerir la inscripción de determinados sistemas de riesgo limitado cuando, por su extensión de uso o su importancia social, estime necesario llevar un control (por ejemplo, un sistema de IA de amplio uso ciudadano que pudiera incidir en opinión pública, o modelos de IA de uso general con potencial efecto sistémico). En tal caso, la Autoridad lo dispondrá motivadamente mediante resolución, definirá la información a inscribir y proporcionará plazos razonables para el registro.
- Publicidad del registro: Por regla general, el Registro de IA será público y accesible, permitiendo a cualquier interesado conocer qué sistemas de IA de alto riesgo están autorizados o en uso en el país, así como sus finalidades básicas. No obstante, se exceptúan de publicidad las partes de la información clasificadas por motivos de seguridad nacional, secreto comercial debidamente justificado o protección de datos personales sensibles. En particular, la inscripción de sistemas de IA utilizados por cuerpos de seguridad del Estado para fines policiales o migratorios no será de acceso público cuando su divulgación pueda comprometer investigaciones o la seguridad (estas inscripciones serán de acceso restringido a las autoridades competentes).
- Actualización y notificación de cambios: Los proveedores o responsables deberán mantener actualizada la información registrada. Cualquier cambio sustancial en el sistema de IA (por ejemplo, nuevo entrenamiento que altere significativamente su desempeño, ampliación de propósito de uso, integración con otros sistemas) deberá notificarse a la Autoridad, que evaluará si requiere una nueva evaluación de conformidad o actualización de obligaciones.
- Colaboración con registros internacionales: La Autoridad podrá coordinar con bases de datos o registros internacionales de sistemas de IA (por ejemplo, la base de datos pública de la UE para IA de alto riesgo) para intercambiar información y buenas prácticas. Asimismo, el registro nacional podrá integrarse en redes de información regional para armonizar estándares y evitar duplicidad de registros cuando un sistema ya conste en registros extranjeros confiables.

El Registro Nacional de IA contribuirá a la transparencia y supervisión democrática de la IA en el país, sirviendo además como fuente de información para la ciudadanía, investigadores y formuladores de políticas.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Artículo 7. Requisitos y Obligaciones para Sistemas de Alto Riesgo. Los sistemas de IA clasificados como de alto riesgo deberán cumplir, previa y posteriormente a su puesta en servicio, con las siguientes condiciones y controles, de conformidad con una IA fiable y centrada en el ser humano:

1. Evaluación de Conformidad Previa: Antes de desplegar o comercializar un sistema de IA de alto riesgo, el proveedor (o quien corresponda) deberá efectuar una evaluación de conformidad para verificar que el sistema cumple con todos los requisitos establecidos en esta ley y sus reglamentos técnicos. Esta evaluación incluirá, entre otros aspectos:

- Calidad de los datos y reducción de sesgos: Demostrar que los conjuntos de datos de entrenamiento, validación y prueba son pertinentes, representativos y con la calidad adecuada en relación con el uso previsto del sistema. Se deberán identificar posibles sesgos en los datos (por ejemplo, subrepresentación de algún grupo poblacional) y adoptar medidas para mitigarlos, a fin de prevenir resultados discriminatorios.
- Documentación técnica y trazabilidad: Disponer de documentación exhaustiva del sistema de IA, que describa su arquitectura general, fuentes de datos, algoritmos utilizados, métricas de desempeño, limitaciones conocidas y supuestos de diseño. Asimismo, el sistema debe incorporar capacidad de registro (logs) de su funcionamiento, para permitir la trazabilidad de sus decisiones o predicciones durante la operación. Esta documentación deberá mantenerse actualizada y estará disponible para la Autoridad bajo solicitud.
- Transparencia y provisión de información: Proporcionar a los usuarios (y a las personas afectadas por el sistema) información clara sobre las características, alcance y limitaciones del sistema de IA. En particular, se informará de modo comprensible qué tarea realiza la IA, su nivel de precisión esperado, las principales variables que influyen en su resultado y las medidas de control humano presentes. Cuando corresponda, se suministrarán también instrucciones de uso seguro, incluyendo recomendaciones para interpretación correcta de los outputs y advertencias sobre posibles errores.
- Supervisión humana: Acreditar que se han incorporado mecanismos para una adecuada supervisión humana del sistema. Esto implica definir las funciones o decisiones que necesariamente estarán a cargo de una persona (y no delegadas enteramente a la IA), los límites dentro de los cuales la IA puede actuar autónomamente, así como las medidas de respaldo o apagado de emergencia ("botón de desconexión" o procedimiento manual) que permitan a un operador humano intervenir y desactivar el sistema en caso de mal funcionamiento o resultados inesperados. Además, los operadores humanos deben recibir capacitación suficiente para interactuar con el sistema de forma segura y efectiva.
- Exactitud, robustez y resiliencia: Demostrar mediante pruebas que el sistema alcanza un nivel apropiado de exactitud, fiabilidad y consistencia en sus resultados, acorde con su finalidad. Asimismo, se evaluará la robustez del sistema frente a variaciones en las condiciones operativas y posibles ataques adversariales. Se deberán implementar salvaguardas para reducir al mínimo resultados erróneos, fallos o incoherencias. En entornos críticos, el sistema debe ser capaz de degradar su funcionamiento de forma segura (por ejemplo, pasando a control manual) ante circunstancias fuera de sus parámetros de diseño.
- Ciberseguridad: Incorporar medidas de seguridad informática que protejan al sistema y sus datos contra accesos ilícitos o manipulaciones intencionadas. Esto incluye



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

controles de acceso, cifrado de datos sensibles, detección de intrusiones, pruebas de penetración regulares, y planes de respuesta ante incidentes. La evaluación debe garantizar que el sistema cumple estándares actualizados de ciberseguridad apropiados para el sector de que se trate.

- Marcado o certificación de conformidad: Si existiesen normas técnicas dominicanas o internacionales aplicables (por ejemplo, normas ISO/IEC para IA) o especificaciones reconocidas, el proveedor podrá adherirse a ellas para demostrar cumplimiento. En caso de ser necesario, la Autoridad o un organismo acreditado podrá emitir un certificado de conformidad del sistema con esta ley. Los sistemas que superen la evaluación satisfactoriamente obtendrán una Declaración de Conformidad expedida por el proveedor, la cual deberá poder exhibirse a requerimiento de las autoridades competentes. (En su caso, se implementará un distintivo o marcado de calidad visible que indique que el sistema ha sido evaluado conforme a la normativa, similar al concepto de marcado CE en la Unión Europea.).

2. Gestión de Riesgos y Calidad Permanente: El proveedor y, en su caso, el responsable del despliegue deberán implementar un sistema de gestión de riesgos y calidad durante todo el ciclo de vida del sistema de IA. Esto incluye: supervisar continuamente el desempeño del sistema en condiciones reales, recoger y analizar las experiencias de uso (feedback), y adoptar sin dilación medidas correctivas si se detectan nuevos riesgos o incumplimientos. Se realizarán evaluaciones periódicas post-comercialización para asegurar que el sistema sigue cumpliendo los requisitos (por ejemplo, reevaluar la exactitud y no discriminación con datos recientes). En particular, si se introducen modificaciones o actualizaciones significativas al modelo o a los datos, deberá repetirse o actualizarse la evaluación de conformidad.

Asimismo, los proveedores deberán establecer canales de reporte para que usuarios o terceros puedan notificar fallos, usos indebidos o incidentes relacionados con el sistema. Estos reportes deberán ser analizados y, de ser graves, comunicados a la Autoridad junto con las acciones tomadas.

3. Obligaciones de proveedores, usuarios y otros agentes: Todos los actores involucrados en la cadena de suministro de sistemas de alto riesgo tienen responsabilidades:

- El proveedor (desarrollador o importador que introduce la IA en el mercado) es responsable principal de la conformidad del sistema con los requisitos antes mencionados. Debe facilitar la documentación técnica completa a la Autoridad cuando sea solicitada, así como la declaración de conformidad y resultados de evaluaciones. Si un proveedor fuera extranjero sin domicilio en el país, deberá designar un representante legal en República Dominicana que actúe en su nombre ante la Autoridad.

- El responsable del despliegue (usuario que opera el sistema en la práctica, por ejemplo una empresa que lo utiliza en su proceso de negocio) deberá utilizarlo conforme a las instrucciones y limitaciones definidas, garantizando la presencia de la supervisión humana establecida. Si este responsable detectare cualquier fallo grave, uso no previsto o riesgo nuevo al emplear la IA, deberá suspender su uso y notificar a la Autoridad inmediatamente. También deberá asegurarse de informar a las personas impactadas por decisiones del sistema sobre sus derechos.

- Los distribuidores o comercializadores de sistemas de IA de alto riesgo deberán verificar que el sistema esté debidamente certificado y registrado antes de ofrecerlo. No deberán suministrar sistemas que saben o debieran saber que no cumplen la ley.

R. Barón



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

•En general, ningún agente podrá modificar un sistema de IA de alto riesgo de manera no autorizada (por ejemplo, cambiando datos o parámetros críticos) sin incurrir en nueva evaluación; de hacerlo, asumirá la responsabilidad como si fuera proveedor de un nuevo sistema modificado.

4.Control previo y autorización especial en ciertos casos: La Autoridad Nacional de IA podrá exigir, para determinados sistemas de alto riesgo de especial sensibilidad (por ejemplo, aquellos usados por el gobierno en decisiones masivas de impacto ciudadano, o innovaciones muy novedosas), una autorización expresa antes del despliegue operativo. Esto podría implicar que la Autoridad revise los informes de evaluación de conformidad, realice pruebas adicionales o solicite la opinión de un comité de expertos o de ética, antes de dar visto bueno a su uso generalizado. El objetivo es añadir una capa de garantía en aplicaciones particularmente delicadas. Esta autorización deberá emitirse en plazos razonables para no entorpecer injustificadamente la innovación

Artículo 8. Obligaciones de Transparencia y Prácticas Leales (AI de riesgo limitado). A fin de proteger a los ciudadanos de engaños o manipulaciones, se establecen medidas de transparencia para ciertos sistemas de IA, incluso si son de riesgo limitado o mínimo, cuando interactúan con personas o generan contenido presentándolo como real:

1.Identificación de interacción con IA: Cualquier sistema de IA (servicio, chatbot, asistente virtual, agente conversacional, etc.) que interactúe con humanos y simule ser una persona o actúe con cierto grado de autonomía, deberá informar claramente a los usuarios que se trata de una inteligencia artificial y no de un humano. Esta revelación debe ser comprensible y ocurrir al inicio de la interacción o en el momento más temprano posible. Por ejemplo, los chatbots que atiendan al público deberán presentarse como asistentes virtuales; si se utilizan voces o avatares sintéticos en lugar de personas, ello debe quedar manifiesto.

2.Notificación de contenidos sintéticos (deepfakes): Toda imagen, audio o video generado o alterado sustancialmente por un sistema de IA, que pueda hacerse pasar razonablemente por contenido real (por ejemplo, videos hiperrealistas de personas diciendo o haciendo cosas que nunca ocurrieron), deberá incorporar una señalización o marca visible/audible indicando que es un contenido artificial. El creador o difusor del contenido sintético será responsable de incluir dicha aclaración (mediante marca de agua, etiqueta textual, disclaimer oral, etc., según el medio). Se exceptúan de este deber los contenidos generados con fines evidentemente artísticos, humorísticos, de parodia o ficción, siempre que su contexto no induzca a error sobre su autenticidad; sin embargo, si tales contenidos se utilizan posteriormente con ánimo de engañar al público en un contexto diferente (por ejemplo, desinformación), esa utilización quedará sujeta a sanción.

3.Transparencia en recomendaciones automatizadas: Las plataformas o servicios que utilicen sistemas de recomendación o personalización mediante IA (por ejemplo, para ofrecer noticias, productos, contenido multimedia personalizado) deberán informar a los usuarios de manera accesible sobre la existencia de algoritmos que filtran u ordenan la información basada en perfiles o preferencias. Además, cuando sea posible, ofrecerán opciones para que el usuario influya en dichas recomendaciones (por ejemplo, indicando sus intereses o eligiendo no recibir personalización).

4.Limitaciones de uso de técnicas engañosas: Queda prohibido utilizar IA para prácticas comerciales desleales o engañosas, tales como bots que difundan masivamente mensajes comerciales haciéndose pasar por opiniones genuinas de consumidores, o



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

algoritmos que manipulen precios individualizados de forma opaca. Tales conductas se considerarán violaciones a la protección del consumidor y a esta ley, y los infractores estarán sujetos a sanciones.

5.Explicabilidad básica al usuario: Sin perjuicio de lo dispuesto para sistemas de alto riesgo, todo proveedor de servicios de IA accesibles al público deberá, a solicitud del usuario, proveer una explicación general del funcionamiento del sistema en términos no técnicos. Esto incluye describir qué datos en general utiliza (sin revelar secretos comerciales), con qué finalidad, y cómo sus salidas pueden afectar al usuario. Asimismo, deberá ofrecer al usuario canales de contacto para consultas o para ejercer sus derechos (por ejemplo, derecho a corrección de datos, etc., conforme a la Ley 172-13 en caso de datos personales).

6.Protección de menores y personas vulnerables: En servicios de IA de interacción pública, se implementarán medidas para detectar y mitigar riesgos para usuarios menores de edad. Por ejemplo, si un asistente virtual detecta que el usuario es un niño, deberá adaptar sus respuestas a contenido apropiado y evitar influencias perjudiciales. Se podrán exigir filtros parentales o verificaciones de edad para cierto tipo de aplicaciones sensibles.

7.Publicidad y etiquetado: Si un sistema de IA es utilizado para crear o difundir contenidos publicitarios personalizados, se informará al destinatario que el contenido fue personalizado mediante procesamiento automatizado. Cualquier anuncio o comunicación masiva generada por IA deberá cumplir la normativa publicitaria vigente, incluyendo identificación del anunciante y veracidad.

Las obligaciones de este artículo buscan asegurar un entorno digital transparente y digno de confianza, donde los usuarios estén debidamente informados cuando contenidos o interacciones son asistidas por IA, evitando engaños y permitiendo tomar decisiones informadas. La Autoridad podrá desarrollar guías específicas sobre cómo cumplir estas obligaciones en distintos contextos tecnológicos.

Artículo 9. Espacios Controlados de Prueba (Sandboxes Regulatorios). Con el fin de estimular la innovación responsable en IA y probar nuevas soluciones tecnológicas de manera segura, la Autoridad Nacional de IA implementará un programa de "sandboxes regulatorios" para IA. Este programa permitirá a organizaciones públicas o privadas, bajo supervisión de la Autoridad, desplegar proyectos piloto de IA innovadores en un entorno limitado y controlado, con exenciones o flexibilidades temporales de ciertos requisitos regulatorios, siempre que se cumplan condiciones estrictas para la protección de los participantes y terceros. Las disposiciones para los sandboxes son:

- Solicitud y selección: Los interesados (empresas, start-ups, centros de investigación, etc.) podrán solicitar a la Autoridad ingresar un proyecto de IA al sandbox, describiendo su innovación, objetivos, riesgos potenciales y salvaguardias propuestas. La Autoridad seleccionará proyectos con alto potencial de beneficio público o desarrollo tecnológico, que requieran flexibilidad regulatoria para ser probados, asegurándose de que no comprometan derechos fundamentales ni la seguridad durante la prueba. Tendrán especial prioridad proyectos enfocados en educación, salud, medio ambiente, cultura, inclusión social u otros sectores de interés nacional.

- Marco contractual y garantías: Antes de iniciar, la Autoridad y la entidad participante firmarán un acuerdo que definirá el alcance del sandbox, las normativas específicas que se flexibilizan, la duración de la prueba, el número y perfil de participantes o usuarios involucrados, las medidas de control y seguridad que se adoptarán, y los criterios de



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

éxito/fallo. Se establecerán asimismo cláusulas de confidencialidad, protección de datos y responsabilidades en caso de daños. Los participantes deberán obtener, si corresponde, el consentimiento informado de usuarios involucrados en la prueba.

- **Monitoreo constante:** Durante la vigencia del sandbox, la Autoridad ejercerá una supervisión cercana del proyecto. Podrá requerir informes periódicos, acceso a resultados interinos, y tiene la facultad de suspender o terminar la prueba de inmediato si advierte riesgos graves no previstos o incumplimientos a las condiciones pactadas.
- **Evaluación final y escalamiento:** Al término del sandbox, la entidad participante presentará a la Autoridad un informe final con los resultados, lecciones aprendidas, riesgos identificados y mitigados, y propuesta de siguientes pasos. La Autoridad evaluará si la innovación probada puede escalarse a operaciones reales y bajo qué condiciones o ajustes regulatorios. En su caso, podrá otorgarse una autorización para su despliegue comercial o uso general, siempre que a partir del sandbox se hayan alineado con los requisitos legales pertinentes. Si el proyecto no alcanzó resultados satisfactorios, la Autoridad procurará que el conocimiento obtenido sirva para guiar futuras iniciativas o ajustar la regulación existente.
- **Difusión de aprendizajes:** Respetando la confidencialidad industrial, la Autoridad publicará conclusiones generales de los proyectos sandbox culminados, con las buenas prácticas y aprendizajes obtenidos, para beneficio del ecosistema de innovación en IA. Estas experiencias podrán informar modificaciones normativas para facilitar la adopción de nuevas tecnologías de forma segura.

El régimen de sandboxes permite combinar la flexibilidad necesaria para la innovación con la protección y supervisión requeridas para salvaguardar el interés público. En todo momento se mantendrá el principio de primacía de los derechos humanos: ninguna experimentación en el sandbox justificará la violación de derechos fundamentales, y cualquier incidente será tratado con rigor, determinándose las debidas compensaciones si alguna persona resultare afectada.

CAPITULO III

GOBERNANZA INSTITUCIONAL Y SUPERVISIÓN

Artículo 10. Autoridad Nacional de Inteligencia Artificial (ANIA). Se crea la Autoridad Nacional de Inteligencia Artificial (ANIA) como el órgano rector encargado de la aplicación de la presente ley, la supervisión del ecosistema de IA en el país y la promoción de su desarrollo ético y seguro. La ANIA será una entidad pública con personalidad jurídica, autonomía técnica, administrativa y financiera, adscrita a efectos administrativos al Poder Ejecutivo (por medio del ministerio u órgano que determine el reglamento), pero con independencia funcional en el ejercicio de sus atribuciones.

La ANIA, también denominada en esta ley como la Autoridad, tendrá las siguientes competencias y funciones principales:

1. **Regulación y Normativa:** Proponer y dictar reglamentos técnicos, estándares y directrices necesarios para la implementación de esta ley. Podrá emitir normas complementarias de carácter general, dentro del marco de la ley, para precisar requisitos técnicos de seguridad, metodologías de evaluación, criterios de clasificación de riesgo u otros aspectos dinámicos. Asimismo, elaborará guías de buenas prácticas



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

para diferentes sectores y promoverá la adopción de códigos de conducta voluntarios en la industria.

2.Registro y Evaluación: Administrar el Registro Nacional de IA (Artículo 6), garantizando su actualización, accesibilidad y correcto funcionamiento. Evaluar las solicitudes de registro y los expedientes de evaluación de conformidad de sistemas de alto riesgo, pudiendo requerir información adicional, realizar verificaciones técnicas o imponer condiciones previas a la inscripción. Tendrá facultad para autorizar o denegar la puesta en servicio de un sistema de IA de alto riesgo si no cumple los requisitos legales, así como para ordenar la suspensión de sistemas ya desplegados que presenten riesgos no tolerables o violen disposiciones de esta ley.

3.Supervisión y Fiscalización: Vigilar el cumplimiento de esta ley por parte de todos los actores (desarrolladores, proveedores, usuarios institucionales, etc.). Para ello, podrá llevar a cabo inspecciones, auditorías técnicas y requerimientos de información. La ANIA tendrá acceso, con las debidas garantías, a los algoritmos, componentes e instalaciones relevantes de los sistemas de IA sujetos a investigación, pudiendo realizar pruebas o simulaciones necesarias para verificar su funcionamiento. Cuando sea pertinente, coordinará operativos de supervisión con otros entes reguladores (por ejemplo, la autoridad de protección de datos, autoridades de competencia, de telecomunicaciones, financiera, etc., según el sector involucrado) para abordajes integrales.

4.Recepción de Denuncias y Quejas: Recibir e investigar las denuncias o quejas de personas, organizaciones o entidades acerca de posibles infracciones a esta ley o riesgos asociados a sistemas de IA. La ANIA establecerá canales accesibles de comunicación para que la ciudadanía pueda reportar preocupaciones, incluyendo mecanismos de denuncia confidencial para informantes internos (whistleblowers) de empresas que adviertan prácticas indebidas. Tras analizar una denuncia, la Autoridad decidirá motivadamente si procede iniciar una investigación formal y en su caso adoptar medidas preventivas.

5.Aplicación de Sanciones: Instruir y resolver procedimientos administrativos sancionadores en caso de incumplimientos, e imponer las sanciones correspondientes conforme al régimen previsto en esta ley (Capítulo VI). La ANIA garantizará el debido proceso en estos procedimientos, incluyendo el derecho de defensa de los presuntos infractores. Sus resoluciones sancionadoras serán fundamentadas y podrán incluir órdenes de cese de conductas, multas, inhabilitaciones temporales, etc., según la gravedad.

6.Orientación y Asistencia Técnica: Prestar asesoría a entidades públicas y privadas sobre la interpretación de la ley y la mejor forma de cumplir sus disposiciones. La Autoridad actuará como referente técnico nacional en IA, difundiendo conocimiento, organizando capacitaciones o foros, y publicando informes periódicos sobre el estado de la inteligencia artificial en el país. Igualmente, asistirá a las instituciones del Estado en la evaluación de soluciones de IA que pretendan adoptar, para asegurar su alineación con los principios de esta ley.

7.Impulso a la Innovación y Cooperación: Gestionar programas de fomento de IA tales como el sandbox regulatorio (Artículo 9), proyectos piloto en colaboración con universidades o empresas, y cualquier fondo de financiamiento asignado para investigación y desarrollo en IA. Podrá celebrar convenios con instituciones académicas, centros de innovación, organismos internacionales y sector privado para



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

ejecutar iniciativas conjuntas que eleven las capacidades nacionales en IA. Asimismo, la ANIA representará al país en redes y foros internacionales sobre gobernanza de IA, cooperando con autoridades homólogas de otras naciones e intercambiando mejores prácticas.

8.Observatorio y Monitoreo Continuo: Actuar como Observatorio Nacional de IA, recopilando datos e informaciones sobre tendencias tecnológicas, adopción de IA en distintos sectores, incidentes o riesgos emergentes, y el impacto socioeconómico de la IA en la República Dominicana. Publicará un informe anual de resultados y hallazgos, incluyendo recomendaciones de políticas públicas o propuestas de actualización normativa para responder a los avances tecnológicos (ver Artículo 16 sobre evaluación continua).

9.Otras atribuciones: Cualesquiera otras funciones que le asignen las leyes o reglamentos, en coherencia con su papel de órgano central en la gobernanza de la IA.

La ANIA contará con el personal técnico y profesional necesario (incluyendo especialistas en ciencia de datos, ética, derecho tecnológico, ciberseguridad, etc.), y podrá crear divisiones internas especializadas (por ejemplo, unidad de evaluación de riesgos, unidad de supervisión sectorial, laboratorio de pruebas). Su estructura, organización interna y recursos serán determinados en el reglamento orgánico correspondiente, asegurando su eficiencia y la no duplicidad de funciones con otras agencias.

Artículo 11. Consejo Nacional de Inteligencia Artificial. Con el objeto de asegurar la coordinación estratégica interinstitucional y la participación de diversos sectores en la definición de políticas sobre IA, se crea el Consejo Nacional de Inteligencia Artificial (CONIA) como órgano consultivo de alto nivel. El CONIA estará integrado por:

- Representantes del sector público: incluyendo, al menos, a un delegado de la Presidencia de la República, los titulares (o representantes designados) de los ministerios vinculados a ciencia y tecnología, educación, industria y comercio, economía/planificación, defensa y seguridad (en lo relativo a ciberseguridad), así como la Dirección de Gobierno Digital u organismo análogo. También se invitará a la Dirección Nacional de Protección de Datos Personales y a la entidad de ciberseguridad del Estado a participar.
- Representantes de la academia y comunidad científica: miembros designados por las principales universidades y centros de investigación del país con experiencia en IA o ética tecnológica.
- Representantes del sector privado: particularmente de las industrias más involucradas en desarrollo o uso de IA (por ejemplo, tecnología, telecomunicaciones, finanzas, salud, manufactura) y de asociaciones empresariales. Se procurará incluir tanto grandes empresas como PYMEs innovadoras.
- Representantes de la sociedad civil: incluyendo ONGs especializadas en derechos digitales, ética tecnológica, protección al consumidor, así como un representante del colegio de abogados o expertos en derecho tecnológico, y otros actores relevantes (por ejemplo, del sector laboral/sindicatos en temas de automatización).

El CONIA será presidido por (la máxima autoridad designada por el Poder Ejecutivo, ej. el Ministro de Ciencia y Tecnología) o quien se determine, y la Autoridad Nacional de IA actuará como secretaría técnica del mismo.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Las funciones del Consejo Nacional de IA incluyen: diseñar la estrategia nacional de IA, emitiendo recomendaciones para incorporar la IA en las prioridades de desarrollo del país; asesorar en la elaboración o actualización de políticas públicas, legislaciones y normativas técnicas relacionadas con IA; servir de espacio de diálogo multisectorial para identificar oportunidades y riesgos de la IA en República Dominicana; promover la colaboración internacional en materia de IA (por ejemplo, asociándose a iniciativas globales de ética en IA, compartiendo conocimientos con otros países); y en general apoyar a la Autoridad brindando perspectivas diversas para la toma de decisiones. El Consejo se reunirá de forma ordinaria al menos dos veces al año y de forma extraordinaria cuando su Presidente lo convoque. Sus recomendaciones no serán vinculantes, pero deberán ser consideradas seriamente por las autoridades competentes; cualquier divergencia significativa deberá ser motivada por escrito.

Adicionalmente, el CONIA supervisará la implementación de la Estrategia Nacional de IA (ENIA) vigente, garantizando su alineación con esta ley y los objetivos de país (como convertir a República Dominicana en un hub regional de IA, conforme a la ENIA). También administrará, con apoyo de la Autoridad, el Fondo Especial de IA indicado en el Artículo 13, determinando prioridades de inversión de acuerdo a dicha estrategia.

Artículo 12. Cooperación Institucional. La ANIA deberá coordinar y cooperar estrechamente con otros órganos reguladores y entidades públicas para una supervisión coherente del ecosistema IA:

- Con la autoridad de protección de datos personales, para asegurar la correcta aplicación de las normas de privacidad en los sistemas de IA y atender conjuntamente reclamaciones o incidentes que involucren tratamiento masivo de datos personales por IA.
- Con la autoridad de ciberseguridad (por ejemplo, el Centro Nacional de Ciberseguridad, una vez establecido mediante la Ley de Ciberseguridad en trámite), para intercambiar información sobre vulnerabilidades de sistemas de IA, amenazas de ciberataques que los involucren, y fomentar estándares de seguridad.
- Con los órganos sectoriales de control (superintendencias, ministerios o agencias especializadas) cuando un sistema de IA incida en sectores regulados: por ejemplo, con la Superintendencia de Bancos para IA en finanzas, con Salud Pública para IA en dispositivos médicos, con Educación para IA educativa, con Trabajo respecto a automatización laboral, etc. Se procurará evitar solapamientos de regulaciones y establecer ventanillas únicas cuando un proyecto de IA requiera múltiples autorizaciones.
- Con el Poder Judicial, facilitando el entendimiento de la tecnología al momento de dirimir disputas legales relacionadas con IA. La ANIA podrá actuar como perito técnico en casos judiciales complejos sobre IA, a requerimiento. También colaborará con el Ministerio Público y fuerzas de seguridad en investigación de delitos que involucren IA (por ejemplo, uso malicioso de deepfakes, ciberataques con IA), dentro del respeto al debido proceso.
- Con organismos internacionales y redes multilaterales: la Autoridad representará al país ante foros como la Red Global de Supervisores de IA, iniciativas de la OCDE sobre IA, esfuerzos de la UNESCO en ética de IA, etc., buscando cooperación técnica y convergencia regulatoria. Podrá suscribir memorandos de entendimiento con homólogas extranjeras para asistencia mutua (por ejemplo, para intercambio de información sobre proveedores foráneos que operen en RD).



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Todas las autoridades públicas dominicanas deberán, en el ámbito de sus competencias, prestar colaboración a la ANIA para el cumplimiento de sus fines, proporcionándole información o recursos cuando les sea requerido de forma razonada.

Artículo 13. Fondo Nacional de Impulso a la IA. Créase el Fondo Especial para el Desarrollo de la Inteligencia Artificial, destinado a financiar iniciativas que promuevan el avance de la IA en el país de manera ética, segura e inclusiva. Este Fondo, de naturaleza pública, será administrado por la Autoridad Nacional de IA bajo la orientación estratégica del Consejo Nacional de IA. Sus características son:

- **Objetivos del Fondo:** i) Incentivar proyectos de IA de alto impacto social en sectores prioritarios (educación, salud, medio ambiente, cultura, seguridad ciudadana, agroindustria, transporte, etc.), ya sean emprendidos por entidades públicas, empresas privadas, academia u organizaciones sin fines de lucro; ii) Fortalecer la investigación y el desarrollo de nuevas tecnologías de IA nacionales, incluyendo apoyo a laboratorios, startups de base tecnológica, programas universitarios y formación de talento; iii) Promover la adopción de IA en PYMEs y sectores tradicionales mediante asistencia técnica y financiera; iv) Fomentar la inclusión digital y la reducción de brechas (por ejemplo, proyectos de IA que beneficien a comunidades rurales, personas con discapacidad, etc.); v) Desarrollar infraestructura crítica para IA, como aumentación de capacidades de cómputo (supercomputación nacional), repositorios de datos abiertos de calidad, plataformas de prueba para desarrolladores locales, etc..
- **Fuentes de financiamiento:** El Fondo se nutre de partidas asignadas anualmente en la Ley de Presupuesto General del Estado (se recomienda un porcentaje específico del PIB tecnológico o de la inversión pública en I+D), recursos de cooperación internacional destinados a IA, contribuciones de empresas nacionales o extranjeras en el marco de convenios (responsabilidad social empresarial enfocada en IA), y hasta un porcentaje de las multas recaudadas por sanciones de esta ley, las cuales podrán ser reinvertidas en acciones de mejora del ecosistema de IA.
- **Modalidades de apoyo:** El Fondo podrá otorgar subvenciones no reembolsables, préstamos blandos, aportes de capital semilla, premios o reconocimientos, así como financiar convocatorias públicas (concursos) para soluciones IA a problemas específicos de desarrollo. Podrá igualmente financiar capacitación de capital humano (becas en ciencia de datos, programas de reconversión laboral hacia habilidades digitales, etc.). Una porción se destinará a mantener los sandboxes regulatorios (cubrimiento de costos regulatorios y apoyo a participantes).
- **Transparencia y control:** La administración del Fondo observará principios de transparencia y rendición de cuentas. Se elaborará un reglamento operativo que establezca criterios de elegibilidad, evaluación de propuestas, composición de comités evaluadores (incluyendo expertos independientes), y mecanismos de monitoreo de la ejecución de los proyectos financiados. Anualmente, la Autoridad publicará un informe de inversiones realizadas, beneficiarios y resultados obtenidos. El Fondo estará sujeto al escrutinio de los órganos de control financiero del Estado (Contraloría, Cámara de Cuentas).
- **Incentivos fiscales asociados:** Adicionalmente, se establecen incentivos fiscales para estimular la inversión privada en IA: por ejemplo, las micro, pequeñas y medianas empresas nacionales que inviertan en la implementación de sistemas de IA responsables podrán acceder a deducciones fiscales o créditos tributarios; igualmente, las empresas extranjeras de base tecnológica que instalen centros de desarrollo de IA en la República



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Dominicana podrían beneficiarse de exenciones o reducciones impositivas temporales, conforme determine la legislación tributaria aplicable. Estos incentivos buscarán posicionar al país como destino atractivo para la innovación en IA, generando empleos de calidad y transferencia de conocimiento.

En conjunto, el Fondo Especial y los incentivos fiscales forman parte de la estrategia de promoción del desarrollo de la IA prevista en esta ley, garantizando recursos y estímulos concretos para materializar los objetivos de progreso tecnológico con equidad.

Artículo 14. Educación, Capacitación e Inclusión Digital. El Estado, con apoyo de la Autoridad y demás instituciones educativas, implementará políticas activas para desarrollar el talento humano en materia de IA y asegurar que la transformación tecnológica sea inclusiva:

- **Currículo educativo:** Se incorporarán contenidos sobre ciencia de datos, programación, robótica e inteligencia artificial en los planes de estudio de la educación básica y media, de forma gradual y acorde al nivel, para preparar a las nuevas generaciones en las competencias del siglo XXI. En la educación superior y técnico-profesional, se fomentará la creación de carreras, asignaturas y certificaciones especializadas en IA, ética tecnológica, análisis de datos y campos afines.
- **Formación continua y reconversión laboral:** El Ministerio de Trabajo, en coordinación con la Autoridad, desarrollará programas de capacitación y re-skilling destinados a la fuerza laboral, especialmente para aquellos empleos que puedan ser transformados significativamente por la automatización y la IA. Se facilitará a trabajadores en sectores vulnerables a la disrupción tecnológica la adquisición de nuevas habilidades para roles complementarios o emergentes en la economía digital. Igualmente, se promoverán alianzas con el sector privado para entrenamientos prácticos (bootcamps, pasantías) en herramientas de IA.
- **Alfabetización digital ciudadana:** Se lanzarán campañas y recursos educativos abiertos para la alfabetización digital e informacional de la población, con énfasis en comprender el funcionamiento básico de la IA, sus potencialidades y riesgos, así como para combatir la desinformación (por ejemplo, cómo identificar deepfakes o contenidos generados por IA). Se prestará especial atención a la inclusión de adultos mayores, poblaciones rurales y otros grupos que puedan tener rezago en adopción tecnológica, asegurando que también se beneficien de las ventajas de la IA.
- **Impulso a la participación de grupos subrepresentados:** En línea con los principios de no discriminación, se articularán iniciativas para que más mujeres y minorías participen en carreras STEM e IA, abordando brechas de género y otras disparidades en el sector tecnológico. Becas específicas, mentorías y redes de apoyo podrán ser establecidas con este fin.
- **Acceso equitativo a la tecnología:** El Estado continuará ejecutando programas para ampliar la infraestructura digital (acceso a internet de banda ancha, dotación de equipos) en todo el territorio, reconociendo que el aprovechamiento de la IA requiere primero cerrar la brecha digital básica. Se velará porque las zonas y comunidades menos desarrolladas no queden rezagadas en la adopción de tecnologías emergentes.

Estas acciones, sumadas a las provisiones del Fondo Especial, tienen como meta final que la revolución de la inteligencia artificial beneficie a toda la sociedad dominicana, potenciando nuestro capital humano y reduciendo desigualdades, en concordancia con los objetivos de la Estrategia Nacional de IA y la Agenda Digital del país



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Artículo 15. Participación en la Formulación de Normas y Estándares Internacionales. El Poder Ejecutivo, a través de la Autoridad Nacional de IA y en coordinación con la Cancillería, deberá promover la participación activa de la República Dominicana en el desarrollo de estándares, principios y acuerdos internacionales relacionados con la inteligencia artificial, la ética digital, la ciberseguridad y temas conexos. En particular, se procurará:

- Adoptar y respaldar los Principios de IA de la OCDE y la Recomendación sobre la Ética de la IA de la UNESCO, entre otros marcos de alto consenso, adecuándolos al contexto nacional.
- Colaborar en esfuerzos regionales (Sistema Interamericano, alianzas iberoamericanas) para la armonización de enfoques regulatorios de IA, reconociendo la naturaleza global de estas tecnologías y la conveniencia de evitar fragmentación normativa que pueda obstaculizar la innovación responsable.
- Participar en foros de normalización técnica (ISO/IEC, IEEE) para contribuir a la elaboración de estándares sobre confiabilidad de algoritmos, calidad de datos, interoperabilidad, etc., asegurando que las perspectivas y necesidades de los países en desarrollo estén representadas.
- Explorar la adhesión a pactos o declaraciones multilaterales sobre IA (como la Global Partnership on AI (GPAI), o iniciativas de cooperación en IA abierta) que puedan ofrecer recursos, conocimiento y colaboración al país.
- Impulsar, en el seno de las Naciones Unidas u otros organismos pertinentes, el debate sobre la gobernanza de IA en ámbitos hoy no regulados internacionalmente (por ejemplo, el uso de IA en conflictos armados, o la protección frente a usos transfronterizos dañinos), abogando por la primacía del Estado de Derecho en las nuevas tecnologías y la responsabilización de los actores privados globales.

La Autoridad Nacional de IA deberá mantener informados periódicamente a los poderes del Estado sobre avances y compromisos internacionales en la materia, recomendando cuando corresponda la actualización de leyes internas o la firma de nuevos tratados.

CAPITULO IV

DERECHOS DE LAS PERSONAS FRENTE A LA IA

Artículo 16. Derechos de los Ciudadanos y Usuarios. Toda persona tiene los siguientes derechos en relación con sistemas de IA, sin perjuicio de otros reconocidos en la Constitución, leyes sectoriales o normativa de protección de datos:

- Derecho a ser informados: Los ciudadanos tienen derecho a saber cuándo están interactuando con un sistema de IA o cuando una decisión que les afecta significativamente ha sido asistida o tomada por una IA. Este derecho se materializa a través de las obligaciones de transparencia establecidas en la presente ley (v.g. aviso de uso de chatbot o de contenido sintético) y en el deber de las entidades de notificar a un individuo si un servicio público o producto privado empleó una IA en la determinación que se adopta hacia él. Por ejemplo, si se deniega un crédito bancario basado en un modelo algorítmico, el individuo debe ser informado de que se utilizó dicha herramienta en la evaluación.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

- Derecho a explicación y revisión humana: En consonancia con el principio de transparencia, toda persona afectada por una decisión significativa basada total o parcialmente en IA podrá solicitar una explicación accesible de los factores y razonamientos generales que condujeron a ese resultado. Igualmente, tendrá derecho a solicitar la revisión humana de dicha decisión, es decir, que una persona con competencia reevalúe su caso sin delegar enteramente en el sistema automatizado. Este derecho es particularmente relevante en ámbitos como selección de personal, concesión de beneficios, sanciones administrativas automatizadas, etc. Las organizaciones deberán establecer procedimientos para atender estas solicitudes en plazos razonables y con la debida diligencia.
- Derecho a la no discriminación algorítmica: Ningún individuo deberá ser sujeto de decisiones automatizadas que resulten en tratos discriminatorios prohibidos por la ley. Si una persona cree haber sido discriminada por el funcionamiento de una IA (por ejemplo, un algoritmo de selección que sistemáticamente rechaza a candidatos de un sexo o etnia), podrá presentar una queja ante la Autoridad Nacional de IA o la instancia correspondiente, la cual investigará el caso. Corresponderá a la entidad responsable del sistema demostrar que no existió discriminación o que se tomaron medidas para prevenirla. De comprobarse sesgo injustificado, el afectado tendrá derecho a la reparación oportuna, incluyendo potencial indemnización según daño causado, sin perjuicio de las sanciones al operador.
- Derecho a la seguridad y al resarcimiento por daños: Las personas tienen derecho a que los sistemas de IA con los que interactúan sean seguros y estén libres de fallos previsibles que puedan causarles daño. Si un sistema de IA (por ejemplo, un dispositivo impulsado por IA) causare daños a una persona (lesiones, pérdidas económicas, violación de sus datos, etc.), la víctima podrá reclamar conforme al régimen de responsabilidad civil aplicable y a lo previsto en esta ley (Art. 20). Los proveedores o usuarios de IA de alto riesgo deberán contar con seguros de responsabilidad u otras garantías financieras para responder por posibles daños, cuando la naturaleza de la actividad lo amerite.
- Derecho a optar por intervención humana: En servicios públicos esenciales, los ciudadanos tendrán derecho, cuando sea viable, a optar por un canal de atención o proceso alternativo que no sea enteramente automatizado. Por ejemplo, si una agencia gubernamental implementa un sistema automatizado para un trámite, deberá ofrecer medios para que quienes así lo prefieran puedan ser atendidos por una persona, al menos durante un período de transición hacia la plena digitalización.
- Derecho a la privacidad y control de sus datos: Conforme a la Ley 172-13, los individuos mantienen el derecho al consentimiento (salvo excepciones legales) para el uso de sus datos personales en sistemas de IA, así como los derechos de acceso, rectificación, cancelación y oposición respecto a dichos datos. En particular, cualquier perfilamiento automatizado realizado mediante IA que produzca efectos jurídicos o impactos significativos en la persona requerirá consentimiento explícito previo, salvo que sea necesario para la ejecución de un contrato o esté autorizado por ley con medidas adecuadas de protección.
- Derecho a no ser objeto de decisiones automatizadas totalmente sin intervención humana en casos sensibles: Este derecho, derivado de los anteriores, implica que decisiones que afecten severamente a alguien (como veredictos legales, diagnósticos médicos vinculantes, etc.) no deben adoptarse únicamente por una IA sin revisión humana apropiada. Si esto ocurriera contraviniendo la ley, la persona tiene derecho a



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

impugnar tal decisión por vía administrativa o judicial, la cual deberá evaluar el fondo del asunto con independencia del resultado producido por la máquina.

- Derecho a la protección frente a la vigilancia indebida: Ningún ciudadano puede ser sometido a vigilancia o monitoreo masivo por sistemas de IA en violación de su intimidad. Cualquier implementación de herramientas de vigilancia basadas en IA por parte de autoridades (por ejemplo, cámaras inteligentes en ciudad) deberá respetar estrictamente los derechos constitucionales y las garantías legales (necesidad, proporcionalidad, autorización judicial cuando aplique). Los ciudadanos podrán recusar o exigir justificación de tales medidas, directamente o a través del Defensor del Pueblo u otro mecanismo.

Los derechos enumerados en este artículo deberán ser garantizados y facilitados por las entidades que desarrollen o utilicen IA. La ANIA velará porque así sea, pudiendo emitir protocolos adicionales para su ejercicio. Estos derechos son de orden público e irre renunciables, y complementan el régimen de protección al consumidor, hábeas data, debido proceso y otros existentes.

Artículo 17. Mecanismos de Reclamo y Acción Judicial. Toda persona u organización que entienda vulnerados sus derechos por el uso de un sistema de IA, o que identifique un incumplimiento de esta ley, podrá recurrir a:

- Reclamo ante la Autoridad Nacional de IA: Presentando una queja o denuncia formal, conforme al Artículo 10 (función de recepción de denuncias). La ANIA investigará los hechos y resolverá lo pertinente, pudiendo ordenar medidas correctivas inmediatas en caso de riesgo grave, e iniciando procedimiento sancionador si corresponde. La ANIA deberá notificar al reclamante sobre el resultado de su gestión en un plazo razonable.

- Procedimientos de mediación o arbitraje: En controversias de índole civil/comercial originadas por sistemas de IA (por ejemplo, disputas contractuales sobre un software de IA defectuoso), las partes podrán voluntariamente someterse a mediación o arbitraje especializados en tecnología, si existieren tales mecanismos en el país, antes o en lugar de acudir a la justicia ordinaria.

- Acción jurisdiccional: Sin perjuicio de lo anterior, el afectado podrá acudir a la jurisdicción contencioso-administrativa si la decisión que impugna proviene de una autoridad pública (ej: una resolución de la ANIA, o una decisión automatizada en un servicio público), o a la jurisdicción civil (o especializada en consumidor, laboral, etc. según el caso) si se trata de un acto de un ente privado, para demandar la protección de sus derechos y la reparación de daños. En estos procesos, los tribunales podrán solicitar peritajes técnicos independientes sobre el funcionamiento de la IA en cuestión.

- Acciones constitucionales: De igual modo, queda a salvo el derecho fundamental de interponer un recurso de amparo en sede judicial constitucional cuando el uso de una IA cause una violación actual o inminente a derechos fundamentales de manera clara. El juez constitucional podrá ordenar la cesación inmediata de la actividad lesiva (por ejemplo, suspender el uso de cierto sistema de IA en el sector público si viola derechos) y otras medidas para restablecer el ejercicio del derecho conculcado.

El Estado fomentará la capacitación de los operadores de justicia (jueces, fiscales, defensores) en materia de IA para asegurar una tutela judicial efectiva en estos novedosos escenarios. En todos los casos, se procurará la resolución ágil de los reclamos dado el rápido avance tecnológico, evitando que la demora procesal torne inútil la protección solicitada.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

CAPITULO V

RÉGIMEN DE RESPONSABILIDADES Y SANCIONES

Artículo 18. Responsabilidad por Daños Causados por IA. Los daños y perjuicios que resulten del desarrollo, provisión o uso de sistemas de IA se regirán por las normas generales de responsabilidad civil, administrativa, penal o laboral según corresponda, con las adaptaciones siguientes para asegurar una adecuada imputación:

- Responsabilidad del proveedor: El desarrollador o proveedor inicial de un sistema de IA será responsable por los daños causados por defectos en dicho sistema (incluyendo errores de diseño, entrenamiento inadecuado o faltas a los requisitos de esta ley), salvo que pruebe que el daño fue causado por el uso del sistema de manera distinta a la prevista o por modificaciones introducidas posteriormente ajenas a su control. Esta responsabilidad del proveedor es de naturaleza objetiva (similar a la responsabilidad por productos defectuosos) cuando se trate de sistemas de alto riesgo colocados en el mercado: deberá indemnizar los daños causados por un mal funcionamiento del sistema, sin que la víctima deba probar negligencia. El proveedor podrá, no obstante, exonerarse total o parcialmente demostrando alguna causal de exoneración aceptada (por ejemplo, fuerza mayor, uso incorrecto por el operador contra las instrucciones explícitas).
- Responsabilidad del operador o usuario: La persona física o jurídica que implementa o utiliza efectivamente el sistema de IA en una actividad (responsable del despliegue) será responsable de los daños que dicha utilización produzca a terceros por falta en el deber de vigilancia, mantenimiento o control humano del sistema. Por ejemplo, si una empresa emplea un algoritmo para tomar decisiones y estas lesionan derechos de un individuo por no haber incorporado la supervisión humana exigida, la empresa responderá por la violación. De igual forma, si un operador utilizó la IA para un fin distinto o en condiciones para las que no fue diseñada, asume la responsabilidad por los daños emergentes.
- Pluralidad de responsables: Cuando concorra culpa o responsabilidad tanto del proveedor como del operador (por ejemplo, un daño ocasionado por una falla de diseño combinada con un uso negligente), ambos responderán frente a la víctima de forma solidaria, sin perjuicio de las acciones de regreso que procedan entre ellos según su grado de contribución al daño. Si intervinieron varios actores en la cadena (fabricante de un componente de IA, integrador, distribuidor, etc.), se determinará caso a caso la cuota de responsabilidad, aplicando el principio de que cada parte asume responsabilidad por la esfera de riesgos que controla.
- Responsabilidad del Estado: El Estado dominicano será patrimonialmente responsable, con arreglo al artículo 148 de la Constitución y leyes especiales, por los daños antijurídicos que puedan causar los sistemas de IA utilizados por sus entidades en servicios públicos o funciones administrativas, siempre que la persona lesionada no tenga el deber jurídico de soportarlos. Sin embargo, el Estado podrá repetir contra el proveedor o funcionario responsable si hubo dolo, culpa grave o incumplimiento a esta ley en la implantación de la IA.
- Seguros y garantías: En sectores de alto riesgo, la Autoridad podrá requerir al proveedor o usuario la contratación de seguros de responsabilidad civil adecuados, fianzas u otras garantías financieras para asegurar la indemnización en caso de eventuales daños



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

causados por la IA (similares a seguros obligatorios de vehículos, trasladado a máquinas autónomas, por ejemplo).

- Causalidad y prueba pericial: Dada la complejidad técnica de los sistemas de IA, en juicios por daños los jueces podrán invertir la carga de la prueba a favor de la víctima una vez que ésta demuestre de forma razonable la plausibilidad de que el sistema de IA tuvo un rol en el daño. Corresponderá al operador/proveedor probar que su sistema no causó el perjuicio o que actuó diligentemente. Se admitirá amplia prueba pericial tecnológica para esclarecer la causalidad (incluyendo inspección del algoritmo si fuera necesario). Si la falta de transparencia del sistema impide conocer las causas del daño, esa incertidumbre perjudicará al responsable, no a la víctima (principio in dubio pro damnato).

- Relación con otras leyes: Lo dispuesto en este artículo complementa el régimen de responsabilidad establecido en la legislación sobre productos defectuosos, defensa del consumidor, código civil, etc., adaptándolo a las particularidades de la IA. En caso de contradicción, prevalecerá la disposición que ofrezca mayor protección a la víctima.

Artículo 19. Infracciones Administrativas. Constituyen infracciones a la presente ley las acciones u omisiones de los sujetos obligados que vulneren sus preceptos. A efectos sancionatorios, las infracciones se clasifican en leves, graves y muy graves:

- Infracciones Leves: Aquellas conductas de escasa significación que implican incumplimientos formales o de bajo impacto. Por ejemplo: no actualizar la información del Registro de IA en plazo; no atender en tiempo un requerimiento de información de la Autoridad; fallas menores en la documentación técnica; incumplimiento parcial de obligaciones de transparencia sin causar perjuicio directo; la primera falta de etiquetado adecuado de un contenido IA sin consecuencias serias.

- Infracciones Graves: Incumplimientos que suponen un riesgo o daño significativo a derechos o a los fines de la ley. Por ejemplo: desplegar o comercializar un sistema de alto riesgo sin haber obtenido la evaluación de conformidad y registro previos; operar un sistema de IA tras haber recibido orden de suspensión; la falta de transparencia deliberada que pueda inducir a error a usuarios (ej. no informar uso de IA en una decisión importante); la resistencia a la supervisión (obstruir inspecciones, falsear u ocultar información relevante a la Autoridad); reincidencia en infracciones leves.

- Infracciones Muy Graves: Violaciones de extrema severidad, que generalmente implican menoscabo cierto a derechos fundamentales, daños generalizados o conducta dolosa. Por ejemplo: el desarrollo o uso de una práctica expresamente prohibida en el Art. 5 (riesgo inadmisible); el incumplimiento intencional de las medidas impuestas a un sistema de alto riesgo que derive en daño efectivo a personas; la negativa reiterada a permitir auditorías de un sistema sospechoso de irregularidades; cualquier uso de IA con fines ilícitos que vulnere gravemente la seguridad pública (por ej., emplear IA para ciberataques, generar desinformación masiva que afecte procesos democráticos, etc.). También se considerará muy grave la omisión de registro de un sistema de alto riesgo (no prohibido) sumada a su puesta en marcha clandestina; o la discriminación sistemática producida por un sistema de IA conocida por el operador y no corregida.

El reglamento podrá detallar supuestos adicionales en cada categoría, atendiendo a criterios de proporcionalidad. Se considerarán factores agravantes la obtención de lucro o beneficio con la infracción, la afectación de un gran número de personas, la reincidencia específica, y la negativa a colaborar; y como atenuantes, la adopción



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

voluntaria de medidas correctivas inmediatas, la colaboración activa para esclarecer los hechos, o que la infracción se cometió por negligencia no grave habiendo intentado cumplir.

Artículo 20. Sanciones Administrativas. La violación de las disposiciones de esta ley dará lugar a la imposición de las siguientes sanciones, según la gravedad de la infracción:

- Para infracciones leves: amonestación por escrito; multas de hasta el equivalente a 100 salarios mínimos del sector público; requerimiento de subsanar el incumplimiento en un plazo fijado bajo apercibimiento de sanción mayor.
- Para infracciones graves: multas desde más de 100 y hasta 5.000 salarios mínimos; suspensión temporal (parcial o total) de las operaciones del sistema de IA involucrado hasta que se garantice su conformidad; publicación de la sanción (para fines ejemplarizantes); inhabilitación para recibir incentivos o financiamiento público en materia de IA por un período dado.
- Para infracciones muy graves: multas desde más de 5.000 salarios mínimos hasta el mayor valor entre 30 millones de dólares estadounidenses o el 6% del volumen de negocios global anual del infractor (para el ejercicio fiscal anterior) ☒, cuando se trate de empresas de gran envergadura; la cifra exacta se fijará considerando la capacidad económica del sancionado y el daño causado. Además, podrá imponerse la prohibición de operar o usar el sistema de IA de manera definitiva en el territorio nacional (veto), la suspensión de actividades relacionada con IA hasta por 5 años, y la inclusión en una lista pública de entidades no confiables en IA. En casos extremos de peligro para la vida o integridad de las personas, la Autoridad podrá proceder al decomiso o destrucción del sistema de IA ilícito.

Las sanciones mencionadas podrán imponerse de forma acumulativa si concurren varios ilícitos. Las multas serán efectivas sin perjuicio de la obligación del infractor de indemnizar los daños causados (responsabilidad civil) e independientemente de eventuales responsabilidades penales. Los ingresos por multas se destinarán preferentemente a financiar las actividades de supervisión de la Autoridad y el Fondo Especial de IA, según lo indicado en el Art. 13.

Previo a sancionar, se seguirá un procedimiento administrativo con audiencia del interesado, garantizando sus derechos de defensa y recurso. Las resoluciones de la Autoridad que impongan sanciones podrán ser recurridas en reconsideración ante la misma y jerárquicamente ante [la instancia superior designada, p. ej., el Ministerio], y en última instancia podrán ser impugnadas ante la jurisdicción contencioso-administrativa para su revisión judicial.

Artículo 21. Medidas Cautelares y Correctivas. En cualquier momento, si la Autoridad Nacional de IA advierte que un sistema de IA o una práctica asociada representa un riesgo grave e inminente para la seguridad, la salud pública o los derechos de las personas, podrá ordenar de oficio medidas provisionales para prevenir daños mientras se sustancia la investigación o procedimiento sancionador. Tales medidas incluyen, entre otras:

- Requerir la suspensión inmediata del funcionamiento o uso del sistema de IA en cuestión, ya sea de forma total o respecto a ciertos contextos o poblaciones vulnerables.



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

- Asegurar pruebas: por ejemplo, incautación temporal de equipos, copias del algoritmo o registros de decisión, para analizarlos técnicamente y evitar su alteración.
- Advertir al público sobre los riesgos de un sistema de IA, mediante comunicados o alertas si la situación lo amerita (por ej., si se descubre un software fraudulento que se esté difundiendo a usuarios).
- Imponer al infractor la adopción urgente de actualizaciones o parches específicos al sistema para cerrar vulnerabilidades de seguridad críticas, bajo supervisión.
- En casos de tratamientos ilícitos de datos personales, coordinar con la autoridad de datos la bloqueo, supresión o secuestro de dichos datos mientras se decide el fondo del asunto.

Estas medidas cautelares se notificarán debidamente y podrán ser recurridas, pero el recurso no suspenderá su ejecución si de ello depende evitar un mal mayor. La Autoridad levantará o ajustará la medida tan pronto cese el motivo de urgencia que la justificó.

Por otro lado, cuando concluya un procedimiento, la Autoridad puede imponer medidas correctivas complementarias junto con o en lugar de sanciones, tales como: la obligación de notificar individualmente a las personas afectadas por una infracción (por ejemplo, informar a usuarios que sus datos fueron expuestos por fallo de IA); la realización de auditorías periódicas independientes pagadas por el infractor para verificar su cumplimiento futuro; la eliminación segura de datos indebidamente recolectados; la publicación de un resumen de las decisiones para transparentar lo ocurrido; la capacitación obligatoria del personal del infractor en ética y normativa de IA, etc. Estas medidas buscan restablecer la legalidad y evitar la repetición de la falta.

Artículo 22. De la Autoridad o por cualquier otra vía resultare que el uso de un sistema de IA se ha vinculado a la comisión de delitos tipificados (por ejemplo, fraude, delitos contra la intimidad, ciberdelitos, falsedad documental mediante deepfakes, incitación al odio automatizada, etc.), la Autoridad dará parte al Ministerio Público para las acciones penales que correspondan. La presente ley no introduce nuevos delitos específicos de IA, pero deja a salvo la aplicación de las figuras penales existentes cuando corresponda.

En particular, se recuerda que: la manipulación dolosa de sistemas informáticos puede constituir delito de sabotaje o daños informáticos; la generación y difusión deliberada de desinformación masiva podría encuadrarse en delitos contra el honor o el orden público dependiendo del caso; el uso de IA para vulnerar sistemas de seguridad es un agravante en delitos informáticos; y la utilización de datos personales sin consentimiento puede conllevar ilícitos penales bajo la Ley 172-13 en caso de violación grave de la privacidad.

Asimismo, los funcionarios públicos que, haciendo uso de sistemas de IA, violen derechos fundamentales o desobedezcan órdenes judiciales, incurrirán en las responsabilidades penales y administrativas que prevean las leyes (como abuso de autoridad, violación de datos, etc.). La Autoridad colaborará como perito o asesor técnico en los procesos penales derivados de estos hechos cuando sea requerida.

CAPITULO VI

DISPOSICIONES FINALES



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

Artículo 23. Evaluación y Actualización Continua. Dada la rápida evolución de la tecnología de IA, el marco jurídico establecido por esta ley deberá ser objeto de evaluación periódica y actualización para garantizar su eficacia y pertinencia. A tal fin:

- La Autoridad Nacional de IA elaborará, cada dos (2) años contados a partir de la entrada en vigor de la ley, un Informe de Evaluación que analice: el grado de cumplimiento e impacto de la ley; avances tecnológicos relevantes ocurridos en ese periodo (ejemplo aparición de nuevas técnicas de IA no contempladas inicialmente); desafíos o lagunas regulatorias identificadas; comparativas con estándares internacionales emergentes; y recomendaciones concretas de reforma si las hubiere. Este informe se presentará al Poder Ejecutivo y al Congreso Nacional, y se hará público para debate de la ciudadanía.
- Se instituye una Comisión de Revisión integrada por representantes de la Autoridad, del Consejo Nacional de IA, juristas, tecnólogos y miembros de las comisiones legislativas competentes, la cual se activará tras cada informe bienal mencionado. Dicha comisión valorará las recomendaciones y preparará, en su caso, un anteproyecto de modificación legislativa para adaptar la ley a las nuevas realidades, sin menoscabo de los principios fundacionales.
- Igualmente, la Autoridad podrá proponer al Poder Ejecutivo reformas puntuales o reglamentarias en cualquier momento si detecta amenazas inminentes que requieren respuesta normativa urgente (por ejemplo, para prohibir una nueva práctica dañina no prevista o para facilitar la adopción de cierta tecnología beneficiosa eliminando trabas). El Poder Ejecutivo podrá dictar reglamentos provisionales al respecto en tanto el Congreso conoce de la materia, siempre dentro del marco de habilitación legal y respetando derechos.
- Se fomentará la participación ciudadana y de expertos en los procesos de actualización: por ejemplo, mediante consultas públicas abiertas sobre borradores de enmiendas, a fin de que la regulación de la IA siga reflejando un consenso amplio y legítimo en la sociedad dominicana.

La intención de esta cláusula es asegurar que la ley no quede rezagada frente al progreso de la IA. La República Dominicana se compromete a mantener un marco regulatorio dinámico y basado en evidencia, aprendiendo de la experiencia práctica y de la comparación internacional (benchmarking) para perfeccionarse continuamente.

Artículo 24. Cláusula de Prevalencia y Compatibilidad. Las disposiciones de la presente ley prevalecerán sobre cualquier otra de igual jerarquía que la contradiga, en lo relativo a la regulación de la inteligencia artificial. No obstante, esta ley se aplicará sin detrimento ni contradicción de los principios y garantías establecidos en la Constitución de la República Dominicana y en los tratados internacionales de derechos humanos ratificados por el país, los cuales primarán en caso de duda interpretativa. Asimismo, se buscará la interpretación más armónica entre esta norma y otras existentes (por ejemplo, la Ley de Protección de Datos, Ley General de Telecomunicaciones, leyes sectoriales) para evitar lagunas o solapamientos. La Autoridad, en coordinación con las entidades competentes, podrá emitir guías interpretativas conjuntas cuando haya áreas de intersección normativa.

Artículo 25. Reglamentación. El Poder Ejecutivo, a través de la entidad que corresponda y con la participación de la Autoridad Nacional de IA, dictará el reglamento o reglamentos para la adecuada aplicación de esta ley en un plazo no mayor de seis (6) meses a partir de su publicación. Dichos reglamentos desarrollarán aspectos técnicos y procedimentales, incluyendo: criterios detallados de clasificación de riesgo,



SENADO REPÚBLICA DOMINICANA

Rafael Barón Duluc Rijo

Senador Provincia La Altagracia

procedimientos de evaluación de conformidad y certificación, organización interna de la Autoridad (estructura, financiamiento, carrera del personal), protocolos de inspección y sanción, operación del Fondo Especial, esquemas de incentivos fiscales, entre otros aspectos que se estimen necesarios para hacer efectiva la ley.

Mientras se emiten los reglamentos, la Autoridad (o en su defecto el órgano público competente en tecnología) podrá emitir lineamientos provisionales para guiar a los involucrados en el cumplimiento de las disposiciones esenciales de esta ley.

Artículo 26. Vigencia. La presente ley entrará en vigor después de transcurridos doce (12) meses contados desde su publicación en la Gaceta Oficial. Este período de vacatio legis tiene por objeto permitir la adecuación de los distintos actores a las nuevas obligaciones aquí establecidas, la creación y puesta en funcionamiento de la Autoridad Nacional de IA y la emisión de la reglamentación correspondiente. No obstante, la autoridad competente podrá iniciar de inmediato las acciones preparatorias para el registro y certificación voluntaria de sistemas de IA, y los sujetos obligados podrán ir adoptando las medidas de cumplimiento con antelación.

Las disposiciones relativas a la prohibición de prácticas de riesgo inadmisibles (Artículo 5.1) tendrán efecto inmediato desde la publicación de la ley, dada la necesidad de prevenir daños graves a los derechos (ejemplo, nadie podrá alegar el período de adaptación para desarrollar una práctica claramente prohibida como el scoring social o manipulación subliminal, las cuales quedan proscritas ipso jure desde la promulgación).

Artículo 27. Disposiciones Derogatorias. Quedan derogadas o sin efecto todas las normas de igual o menor jerarquía que resulten incompatibles con la presente ley. En particular, (si existiera alguna disposición previa sobre IA o gobernanza digital que contradiga, mencionarla). Se mantiene la vigencia de las disposiciones sectoriales que complementen esta ley siempre que no la contravengan.

Artículo 28. Cláusula Final. Esta ley deberá citarse como la "Ley de Inteligencia Artificial de la República Dominicana" y para su ejecución queda encargada la Autoridad Nacional de Inteligencia Artificial y demás organismos en el ámbito de sus competencias. El Poder Ejecutivo, a través de la entidad correspondiente, realizará las gestiones necesarias para la asignación presupuestaria que requiera la implementación de esta ley desde el siguiente ejercicio económico.

Iniciativa presentada por:

Rafael Barón Duluc Rijo
Senador de la República provincia La Altagracia

