PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE DERECHO Y SACIEDAD

CARRERA DE DERECHO



TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA: REGULACIÓN DE LA RESPONSABILIDAD EN CASO DE VULNERACIÓN DE DERECHOS FUNDAMENTALES GENERADOS POR IA

AUTOR: MARÍA VICTORIA SALVADOR BAQUERO

Quito DM,16 de junio de 2026

Resumen:

La presente investigación analizará la determinación de responsabilidad jurídica frente a las vulneraciones de derechos humanos generadas por el uso de la inteligencia artificial (IA) en el sector público ecuatoriano. En el presente contexto, aún no existe una regulación específica sobre la materia en Ecuador, por lo que, mediante un enfoque comparativo y cualitativo, se analiza el marco normativo y doctrinario, y casos tanto nacionales como internacionales de vulneraciones a derechos humanos generados por IA, para definir la forma más eficiente de atribuir responsabilidad. La investigación busca determinar los sujetos y el medio para responder jurídicamente ante las decisiones automatizadas[1] que afecten derechos fundamentales. De esta forma, se plantea como aumentar la seguridad jurídica acerca de este tema. La relevancia del tema se desprende de los elementos expuestos previamente, especialmente la falta de regulación en el sector público y su involucramiento con posibles violaciones a derechos humanos en casos nacionales que están ocurriendo en la actualidad. Finalmente, esta investigación propone criterios de evaluación para determinar una posible responsabilidad estatal con un efecto bola de nieve inverso para que nadie quede impune.

Palabras clave: responsabilidad, derechos humanos, IA, sector público, Estado

This research analyzes the determination of legal liability for human rights violations arising from the use of artificial intelligence (AI) in the Ecuadorian public sector. In the current context, there is still no specific regulation on this matter in Ecuador. Therefore, through a comparative and qualitative approach, this study examines the legal and doctrinal framework, as well as national and international cases involving human rights violations generated by AI, to determine the most effective way to attribute responsibility. The research seeks to identify the relevant actors and the appropriate mechanisms for establishing legal accountability in cases of automated decisions that affect fundamental rights. In this way, it aims to enhance legal certainty regarding this issue. The relevance of the topic stems from the factors outlined above, particularly the absence of regulation in the public sector and its connection to potential human rights violations in contemporary cases. Finally, this research proposes evaluation criteria to determine the possibility of state liability through an inverse snowball-effect approach, ensuring that no responsible party remains unaccountable.

Key words: Responsibility, human rights, automatized decisions, public sector.

[1] Según Soriano (2021) es el resultado de un proceso realizado por un algoritmo que analiza datos y ejecuta instrucciones para clasificar o predecir comportamientos, produciendo decisiones que pueden generar efectos jurídicos o afectar significativamente los derechos de los individuos.

ÍNDICE:

INTRODUCCIÓN

CAPÍTULO I - IA, DERECHOS HUMANOS Y RESPONSABILIDAD ESTATAL: MARCO TEÓRICO Y NORMATIVO

1.1 La IA y los derechos humanos

1.2 Regulación internacional de la IA

1.3 Los derechos humanos y su vulneración en casos de IA

CAPÍTULO II - RESPONSABILIDAD ESTATAL EN CASOS DE IA

2.1 Regulación de la IA a nivel global

2.2 Estándares para la atribución de responsabilidad derivados de casos internacionales

2.3 Marco jurídico ecuatoriano frente a la IA y evaluación del Proyecto de Ley Orgánica de Regulación y Promoción de la IA

2.4 La brecha de responsabilidad de sistemas de IA en Ecuador

2.5 Criterios para la atribución de responsabilidad estatal en el uso de IA

CAPÍTULO III - IMPLEMENTACIÓN DE RESPONSABILIDAD DE IA EN ECUADOR: CASOS RELEVANTES

3.1 Casos relevantes en Ecuador

3.2 Análisis de los criterios establecidos para la atribución de responsabilidad en los casos relevantes

3.3 Aplicación práctica del Proyecto de Ley en casos relevantes de IA en Ecuador

CAPÍTULO IV - CONCLUSIONES Y RECOMENDACIONES

3.1 Conclusiones

3.2 Recomendaciones

INTRODUCCIÓN:

La inteligencia artificial (IA), definida como el desarrollo de algoritmos[2] y modelos computacionales capaces de realizar tareas que reemplazan la inteligencia humana (Axpe, 2024), se ha consolidado como una de las innovaciones más disruptivas de la historia (Suleng Furió et al., 2025). Sin embargo, sus procesos internos no son visibles para el usuario. Este fenómeno, conocido como "caja negra" o "*black box*"[3], se define como: "cualquier sistema cuyos mecanismos internos son desconocidos o indescifrables, pero cuyo comportamiento puede observarse examinando sus entradas y salidas" (Youvan, 2025, p. 4). Esta opacidad genera riesgos jurídicos en Ecuador, como la vulneración de la igualdad y no discriminación, la protección de datos y la tutela judicial efectiva, derechos reconocidos en la Constitución de la República del Ecuador -CRE y en el bloque de constitucionalidad[4]. Uno de estos derechos se relaciona con la calidad de los datos de entrenamiento, puesto que las vulneraciones pueden producirse cuando dichos datos no representan adecuadamente la diversidad de la población (UN Global Compact Network Germany, 2024, p. 9). En Ecuador, el fenómeno se agudiza en tanto el acceso a información personal está limitado por la Ley Orgánica de Protección de Datos Personales (LOPDP), cuyo artículo primero dispone que su objeto es "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter" (LOPDP, 2021).

El uso de la IA en Ecuador ha incrementado progresivamente hasta alcanzar al sector público. Barragán Martínez (2022) señala que su implementación se intensificó durante la crisis del COVID-19, específicamente en hospitales del Instituto Ecuatoriano de Seguridad Social (IESS), donde un software donado por la empresa China Huawei intentó mejorar el diagnóstico de pacientes con síntomas respiratorios complejos. Este contexto de utilización de la IA se evidenció la necesidad de determinar las posibles vulneraciones de derechos humanos derivadas del su uso en el sector público.

[2] Según Morandín, F.(2022) un algoritmo se define como un conjunto de pasos o reglas que siguen los sistemas automatizados para resolver un problema o realizar una tarea específica.
[3] Según Hassija et al(2024) Los modelos de black box realizan predicciones a partir de datos de entrada, pero el razonamiento que conduce a esas predicciones no es transparente para el usuario, lo que dificulta comprender su comportamiento o detectar errores y sesgos.
[4] Este integra a la Constitución y los tratados internacionales de derechos humanos con jerarquía constitucional, que sirven como parámetro para controlar la validez de las normas. Según el artículo 424 de CRE, los tratados de derechos humanos ratificados por el Estado prevalecen sobre el resto del ordenamiento jurídico.

Lo que delimita el tema central de esta investigación es la responsabilidad estatal frente a vulneraciones de derechos humanos por sistemas de IA usados en el sector público. Para sustentarlo, se analizarán las normas nacionales e internacionales aplicables, los criterios que vinculan al Estado con los actores privados involucrados y los mecanismos de reparación disponibles. La hipótesis de esta investigación sostiene que el Estado debe responder mediante un régimen de responsabilidad directa e indirecta, en virtud de su deber de garantía y protección de los derechos humanos. Esto será verificado mediante una metodología cualitativa y comparativa orientada a identificar criterios jurídicos comunes y divergentes en contextos donde el uso de IA derive en afectaciones a derechos fundamentales.

El objeto de esta investigación es proponer criterios para determinar la responsabilidad jurídica[5] en Ecuador frente a vulneraciones de derechos humanos derivadas del uso de IA en el sector público. Para ello, el análisis se estructura en torno a tres variables jurídicas interrelacionadas. La primera es el titular de la responsabilidad, que identifica al obligado a responder frente al ciudadano, ya sea el Estado, el proveedor privado o ambos. La segunda es el hecho generador, que delimita cuándo surge la obligación de responder, entendido como la decisión automatizada que cause daño y vulnere un derecho fundamental. La tercera es la reparación integral, que define las consecuencias jurídicas tras la vulneración, como el conjunto de medidas para restablecer los derechos afectados. Bajo este enfoque, la investigación examina cómo la opacidad y la falta de control sobre esta pueden afectar en servicios públicos, lo que hace necesario precisar la metodología en la que se basará la presente investigación para llegar a la hipótesis central de la misma.

Para alcanzar dicho objetivo, se adoptará una metodología comparativa:

> Esta se entiende como aquella en la que el investigador selecciona dos o más unidades de igual valor con el propósito de analizarlas mediante la identificación de elementos comunes y/o discordantes, lo que permite explicar por qué determinados resultados se presentan o no en cada caso. (Circona, 2023, p.34)

[5] Según Vélez Vélez (2015) es el estado en el que una persona queda sujeta a una posible sanción por la comisión de un acto ilícito, como consecuencia del incumplimiento de una norma jurídica.

Este enfoque se aplica mediante el análisis del marco jurídico ecuatoriano, los estándares del sistema interamericano de derechos humanos, el AI Act[6] la Encíclica del Papa León XIV Magnifica Humanitas como referentes morales internacional y casos de IA y DDHH en el mismo ámbito. El sistema interamericano resulta vinculante para Ecuador en tanto el país ha ratificado los tratados que lo conforman; el derecho ecuatoriano es el ordenamiento analizado, cuya falta de regulación específica sobre IA constituye el problema central de la investigación; el AI Act se incorpora como referente comparado no vinculante, por ser el marco normativo más desarrollado en materia de responsabilidad por sistemas de IA a nivel mundial. El criterio transversal que hace comparables estos tres sistemas es que todos reconocen obligaciones estatales frente a vulneraciones de derechos fundamentales, establecen estándares de atribución de responsabilidad y prevén mecanismos de reparación.

De igual manera, se empleará un método cualitativo, entendido como aquel que formula inferencias generales a partir de una idea desarrollada en la investigación (Circona, 2023). Será aplicado mediante el análisis doctrinario, normativo y jurisprudencial sobre responsabilidad.

La investigación tendrá la siguiente estructura: en primer lugar, los fundamentos teóricos y las implicaciones de la normativa ecuatoriana en materia de responsabilidad y manejo de datos con mecanismos automatizados. En segundo lugar, la información obtenida que será contrastada con el derecho ecuatoriano e internacional para definir las bases jurídicas de atribución de responsabilidad, para finalmente formular recomendaciones orientadas a establecer límites claros, garantizar el acceso a datos gestionados éticamente y reducir el riesgo de decisiones automatizadas que deriven en vulneraciones de derechos humanos.

CAPÍTULO I - IA, DERECHOS HUMANOS Y RESPONSABILIDAD ESTATAL: MARCO TEÓRICO Y NORMATIVO

A continuación, se desarrollará el marco teórico de la presente investigación. Este, según Trigo-Soto (2021) constituye la base conceptual de un estudio. Además, Salinas-Atausinchi, et.al (2023) proponen que el marco teórico debe conformar el sustento y fundamento de la investigación, que articula teorías y conocimientos sobre el problema a estudiar. De manera que el

[6] El IA Act (Reglamento de Inteligencia Artificial) es la primera ley integral del mundo creada para regular esta tecnología, asegurando que su uso sea seguro y respete los derechos fundamentales de las personas, creada en Europa. (Parlamento Europeo y Consejo de la Unión Europea, 2024)

análisis conceptual se conduce desde la IA y los derechos humanos, hasta el desglose de responsabilidades que pueden surgir. Metodológicamente, se basa en un enfoque cualitativo y comparativo, sustentado en la revisión normativa, doctrinal y jurisprudencial que llevan a la determinación de dicha responsabilidad al evaluar el punto de convergencia de los factores que causan el problema a estudiar.

1.1 La IA y los derechos humanos

En un mundo de constante evolución tecnológica, la IA, mejor entendida como: "el uso de algoritmos y tecnologías de aprendizaje automático para permitir que las máquinas imiten ciertas capacidades cognitivas y realicen tareas de manera autónoma o semiautónoma" (Morandín, 2022, p. 3), plantea desafíos relevantes para la protección de los derechos humanos, especialmente cuando esta los transgrede. Por lo que al dejar que la IA maneje algo tan delicado la convierte en un peligro. Al someter DDHH en un espacio cibernético[7] cuyo funcionamiento no puede ser controlado ni comprendido directamente por las personas usuarias[8], llena de incertidumbre a las personas quienes sus derechos se ven involucrados. Petch y Nelson (2022) sostienen que este espacio, denominado "*black box*", constituye un mecanismo de aprendizaje de tal complejidad que su lógica interna no puede ser entendida de manera directa. Esto genera incertidumbre cuando se involucran estos derechos, en tanto resulta imposible identificar con claridad el origen del error y el responsable de la vulneración. En esa misma línea, el Global Compact Network Germany (2024) señala que la opacidad y la falta de trazabilidad[9] en el procesamiento de datos incrementan el riesgo de afectaciones a derechos fundamentales, que dificultan tanto la atribución de responsabilidad como el acceso a mecanismos de reparación.

Este fenómeno, conocido como *black box*, según Izaurieta y Saavedra (s.f.), ocurre entre los inputs[10] y los outputs[11], cuando la IA procesa la información mediante nodos[12] o neuronas artificiales que combinan datos con pesos matemáticos para generar un resultado, sin que sea

[7] Según el Proyecto de Ley Orgánica para el Fortalecimiento de la de Ecuador (2026), es un entorno global compuesto por infraestructuras de tecnologías de la información, redes de comunicaciones, sistemas y dispositivos interconectados.
[8] Según el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador (2024), los usuarios finales pueden ser tanto personas como organizaciones que utilicen el sistema de IA.
[9] Según el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador (2024) es la capacidad de registrar, documentar y auditar todas las etapas del ciclo de vida de un sistema de IA.
[10] Es la señal inicial que ingresa a un sistema de IA para ser procesado y transformado en un resultado. (Izaurieta, y Saavedra, s.f.)
[11] Es la señal de salida generada por neurona artificial tras recibir y transformar los datos de entrada. (Izaurieta, y Saavedra, s.f.)
[12] Es la unidad fundamental de una red, cuya función y representación varía según el contexto técnico. (Izaurieta, y Saavedra, s.f.)

posible entender claramente cómo llegó a esa conclusión. La información pasa por varias capas ocultas que la transforman de forma compleja, que generan opacidad, ya que, aunque el proceso es matemático, "mucho de la complejidad de la operación del modelo permanece sin contabilizar" (Petch et al., 2022, p. 210). Esta falta de control sobre las fuentes y la pérdida de consistencia conceptual[13] durante el procesamiento de los datos genera las alucinaciones de la IA. Según Artopoulos y Lliteras (2024), este fenómeno surge por una "dilución epistemológica del control de fuentes" (p. 1), que lleva al modelo a completar vacíos con patrones estadísticos, que generan respuestas falsas pero coherentes que resultan difíciles de distinguir de la verdad.

La IA maneja datos a través de redes neuronales profundas[14] llamadas "*deep learning*"[15] como menciona Valle, et. Al. (2025), que, además, sostiene que este permite a la IA aprender automáticamente características relevantes. De manera que mientras más información se le entrega, es menor el riesgo de discriminación. De manera análoga, es importante señalar que, aunque la IA procesa datos y aprende características de forma autónoma, también genera errores y "alucina"[16].

Definido esto, se puede notar la imposibilidad de identificar el momento preciso en el que la IA alucina y genera errores (nexo causal[17]). De manera que, si la IA estuviese manejando datos que involucren DDHH en la administración pública, no se podría identificar en qué momento o en que nodo ocurrió la alucinación que generó la vulneración, por lo que causaría incertidumbre acerca del nexo causal, el cual es uno de los requisitos que exige el Código Orgánico Administrativo (COA) (2017) para atribuir responsabilidad extracontractual (art. 331. 3). En consecuencia, tampoco se cumplirían garantías del debido proceso previstas en el art. 76 No. 3 de la CRE (2008), que exige la existencia de una norma previa, y el No. 7 literal e, que obliga a motivar las decisiones con base en hechos y normas claras. Asimismo, se configura una imposibilidad probatoria, pues el Código Orgánico General de Procesos (COGEP) (2026, art. 158) establece que la prueba debe generar convicción en el juzgador, lo cual no es viable sin comprender

[13] Según Artopoulos, y Lliteras (2024) es la coherencia lógica y la integridad de las ideas que un modelo de IA mantiene al generar una respuesta.
[14] Son estructuras con múltiples capas que imitan, de forma simplificada, el funcionamiento del cerebro humano.
[15] Es una metodología de IA basada en redes neuronales que aprende automáticamente características a partir de los datos (Valle, et. al., 2025).
[16] La generación de información falsa o engañosa que resulta difícil de distinguir de la información considerada verdadera (Artopoulos, y Lliteras, 2024)
[17] Artículo 335.- Nexo causal. El nexo causal entre el daño calificado y la acción u omisión de la administración pública o el hecho dañoso que violente el derecho se fundamentará en hechos probados. (COA, 2017)

el origen del error. De este modo, la opacidad de la IA dificulta probar los hechos, atribuir responsabilidad y garantizar mecanismos efectivos de control y reparación frente a vulneraciones de derechos humanos.

1.2 Regulación internacional de la IA

Ante este escenario, la gobernanza global de la IA ha evolucionado más allá de marcos regionales. Si bien la Unión Europea (2024) estableció un precedente de "*hard law*"[18] mediante el "AI Act" para garantizar derechos fundamentales, este se complementa con instrumentos de "*soft law*"[19] de alcance universal. El Pacto Digital Global de la ONU (2024) y las Recomendaciones sobre la Ética de la IA de la UNESCO actúan como marcos de referencia que integran la soberanía de datos y la transparencia algorítmica. Estos organismos, junto con los estándares técnicos de la ISO/IEC 42001[20] (2023), configuran un sistema de gobernanza donde la norma internacional técnica precede y fundamenta la obligatoriedad de las leyes nacionales.

El AI Act (2024) regula los usos de sistemas automatizados según su impacto en derechos fundamentales, clasificándolos en cuatro niveles de riesgo (punto No. 26): inaceptable (prohibido), alto (con requisitos estrictos), limitado (con obligaciones de transparencia) y mínimo (sin regulación adicional). En materia de responsabilidad, el reglamento distingue entre proveedores y responsables del despliegue[21]. Los primeros están obligados a mantener actualizado el sistema y remitir documentación técnica a las autoridades competentes, bajo sanción en caso de incumplimiento (AI Act, 2024, art. 101). Los segundos deben realizar evaluación de impacto (art. 27 [22]) sobre derechos fundamentales antes de desplegar un sistema de IA, por ser un sistema de alto riesgo[23]; de modo que se cumplan las obligaciones de transparencia[24]. Finalmente, el Estado

[18] Según Zambrano Pérez, D. A. (2019), este comprende normas de carácter obligatorio y vinculante dentro de un sistema jurídico.
[19] Se compone de reglas que "sirven como guía de interpretación de las primeras, pues dotan de mayor precisión a los contenidos mínimos fijados convencionalmente" (Corte Interamericana de Derechos Humanos, 2017, p. 32).
[20] La norma ISO/IEC 42001 es un estándar internacional diseñado específicamente para establecer, implementar, mantener y mejorar un Sistema de Gestión de Inteligencia Artificial (SGIA).
[21] Es quien utiliza un sistema de IA bajo su propia autoridad en un contexto profesional (AI Act, 2024, art. 3.4).
[22] Obligación de analizar, antes de usar un sistema de IA de alto riesgo, los riesgos sobre derechos fundamentales y definir medidas para mitigarlos (AI Act, 2024, art. 27).
[23] Según el Reglamento (UE) 2024/1689 (AI Act), es aquel que tiene un efecto perjudicial considerable en la salud, la seguridad o los derechos fundamentales de las personas en la Unión Europea.
[24] Obligación de informar a las personas cuando interactúan con un sistema de IA y de etiquetar los contenidos generados artificialmente, como los deepfakes, para evitar el engaño (AI Act, 2024).

debe garantizar supervisión humana efectiva y cumplir obligaciones de transparencia y alfabetización[25] en la IA (AI Act, 2024, art. 27).

No obstante, el análisis comparativo entre el AI Act y el derecho ecuatoriano evidencia tanto compatibilidades normativas como barreras estructurales en su aplicación. Como punto de convergencia, el derecho al obtener una explicación "cuando la decisión de un responsable del despliegue se base principalmente en los resultados de salida de determinados sistemas de IA de alto riesgo" (AI Act, 2024, punto 171)[26] es trasladable al Ecuador, donde la LOPDP ya reconoce la facultad del titular de "solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada" (art. 4, inc. 4). Sin embargo, la implementación de una autoridad centralizada de supervisión enfrenta límites en la CRE, que dispone que las instituciones del Estado "ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley" (CRE, 2008, art. 226), lo que dificulta una gobernanza transversal[27] sin reformas constitucionales. De igual forma, la escala de sanciones del modelo europeo contrasta con la rigidez del ordenamiento ecuatoriano, que establece multas para funcionarios públicos de "entre 10 a 20 salarios básicos unificados" (LOPDP, 2021, art. 72), frente a grandes proveedores tecnológicos. En consecuencia, se identifican tanto espacios de armonización normativa como brechas relevantes que demuestran que, para que una norma regule la IA en Ecuador, debe ser compatible con el contexto del país y sus normas.

1.3 Los derechos humanos y su vulneración en casos de IA

Los derechos humanos no se reducen a un conjunto de normas dispersas en diversas legislaciones, sino que constituyen un sistema coherente de garantías y derechos fundamentales que aseguran una vida digna para todas las personas. La Corte Interamericana de Derechos Humanos (CIDH) (2025) en la Opinión Consultiva OC-32/25 sostiene que los derechos humanos se fundamentan en los atributos inherentes a la persona y su dignidad esencial, siendo por tanto inalienables para todos los individuos sin distinción de raza, nacionalidad, credo o sexo (p. 8). En

[25] La alfabetización en IA comprende los conocimientos necesarios para comprender su funcionamiento, evaluar sus oportunidades y riesgos, y entender las repercusiones de las decisiones automatizadas (AI Act, 2024).
[26] Se compone de reglas que "sirven como guía de interpretación de las primeras, pues dotan de mayor precisión a los contenidos mínimos fijados convencionalmente" (Corte Interamericana de Derechos Humanos, 2017, p. 32).
[27] Según la Asamblea Nacional (2024) se refiere a un modelo de supervisión y control donde los principios rectores, obligaciones y salvaguardas de la inteligencia artificial no se aplican de forma aislada, sino que se integran en todos los sectores, niveles organizativos y procesos de gestión.

este sentido, la siguiente tabla tiene como objetivo sistematizar el concepto de vulneración de derechos humanos y los elementos que configuran su existencia en distintos sistemas jurídicos. No obstante, su principal aporte radica en vincular estos criterios teóricos con casos concretos de implementación de IA, que evidencian cómo dichos estándares se materializan en escenarios reales.

Tabla 1.

Derechos humanos, violación y constitución de la violación de DDHH en casos de IA

Norma / Instrumento	Qué se entiende por derechos humanos	Qué se considera violación de derechos humanos	Cómo se constituye una violación de derechos humanos	Ejemplos de IA como ente vulnerador
Sistema Interamericano (Convención Americana Sobre Derechos Humanos)	Los derechos humanos son derechos inherentes a todas las personas, no otorgados por el Estado, universales e inalienables, que comprenden desde el derecho a la vida hasta derechos que hacen la vida digna, como salud, educación y libertad (Office of the High Commissioner for Human Rights [OHCHR], s. f.-a).	Hay violación cuando actos u omisiones imputables al Estado desconocen o restringen injustificadamente los derechos reconocidos en la Convención, incumpliendo el deber de "respetar" y "garantizar" el libre y pleno ejercicio de esos derechos (OAS, 1969/1978, art. 1).	Se configura una violación cuando concurren, al menos: (1) existencia de un derecho protegido por la Convención; (2) conducta u omisión estatal contraria a ese derecho; (3) falta de medidas de garantía o prevención suficientes; y (4) inexistencia o ineficacia de recursos internos para reparar el daño, según ha desarrollado la jurisprudencia interamericana sobre la obligación de respetar y garantizar (OAS, 1969/1978).	En Argentina se evidencia una posible vulneración de derechos humanos; privacidad, protección de datos, no discriminación, derecho a la defensa y tutela judicial efectiva. El sistema "Gemelo Digital Social" por parte del Ministerio de Capital Humano busca predecir el impacto de políticas públicas mediante el procesamiento masivo de datos haciendo una simulación de distintos escenarios para ver el impacto que podrían tener, lo que lo convierte en un "Estado predictivo" según Chaves (2026). Argentina no tiene una norma general que regule este tipo de tecnología de alto impacto en derechos humanos. Por lo que la vulneración se constituiría por la acción estatal de procesar información privada mediante una "caja negra" que posee "imposibilidad probatoria".
Sistema europeo (Convenio Europeo de	Los derechos humanos se conciben como derechos inherentes	El TEDH determina que una violación de derechos humanos es cuando	La violación se constituye cuando: (1) un derecho protegido	En los Países Bajos se evidenció una vulneración de derechos humanos, particularmente del

Derechos Humanos + estándares Consejo de Europa)	a toda persona, protegidos por el Convenio Europeo y otros instrumentos, que actúan como "armadura", "reglas" y "jueces"; estos derechos pertenecen a todas las personas sin distinción (Council of Europe, 1950).	el Estado parte incumple las obligaciones del Convenio Europeo de Derechos Humanos y sus Protocolos, que afectan así los derechos y libertades que estos instrumentos consagran. (Council of Europa, 1950)	por el Convenio es afectado; (2) ha ocurrido un acto u omisión por el estado parte; (3) hay una afectación del derecho protegido; y (4) debe haber un acceso efectivo a los recursos. Estos elementos son claves para que el Tribunal Europeo declare una vulneración de DDHH. (Council of Europe, 1950)	derecho a la vida privada y a la no discriminación, derivada del uso del sistema SyRI. Esta afectación se originó en una acción estatal, al implementar un sistema de detección de fraude que operaba de forma opaca y focalizada en sectores vulnerables, así como en una omisión, al no establecer mecanismos adecuados de transparencia, control y evaluación. A ello se suma la falta de regulación específica y garantías suficientes de aquella época. (Muñoz Ruiz, 2020)
Normativa ecuatoriana (Constitución de la República del Ecuador + desarrollo interno)	La Constitución del Ecuador establece que los derechos reconocidos en ella y en los instrumentos internacionales son de aplicación directa, inalienables, irrenunciables, interdependientes, indivisibles, e inherentes a todas las personas y comunidades, que obligan al Estado a garantizarlos sin discriminación (República del Ecuador, 2008, arts. 3 y 11; Ministerio de Gobierno, 2012)	Hay violación cuando una autoridad, por acción u omisión, desconoce, restringe u obstaculiza el goce efectivo de un derecho reconocido en la Constitución o en instrumentos internacionales, incumpliendo el deber primordial del Estado de garantizar su ejercicio sin discriminación (República del Ecuador, 2008, art. 3).	Se constituye la violación cuando: (1) existe un derecho constitucional o convencional aplicable; (2) se verifica una acción u omisión estatal que lesiona ese derecho; (3) se incumplen las obligaciones de respeto, protección y garantía; y (4) no se provee un recurso judicial efectivo ni una reparación adecuada, lo que habilita el uso de garantías jurisdiccionales como la acción de protección (República del Ecuador, 2008) y (Ministerio de Gobierno, 2012).	En Ecuador, el uso de IA en el sistema judicial puede configurar una vulneración de derechos humanos, especialmente del debido proceso y la garantía de motivación. En primer lugar, existe un derecho constitucional aplicable que exige decisiones judiciales fundamentadas. En segundo lugar, se verifica una acción estatal al incorporar estas tecnologías y una omisión al carecer de regulación específica. En tercer lugar, la opacidad algorítmica y la posible reproducción de sesgos evidencian un incumplimiento de las obligaciones de garantía. Finalmente, la falta de explicabilidad[28] limita la impugnación de decisiones, que afectan la efectividad de los recursos judiciales y la reparación. (Narváez, Vaca, Escobar y Campos, 2025)

[28] El IA Act (2024) establece que las personas afectadas por una decisión basada en sistemas de IA de alto riesgo tienen el derecho a recibir explicaciones claras y significativas sobre el papel del sistema en el proceso de toma de decisiones y los elementos principales que llevaron a dicha conclusión.

Fuentes: Mixtas

A partir del cuadro comparativo se identifica que los tres sistemas los derechos humanos son universales, inherentes y de obligatoria garantía por parte del Estado, cuya vulneración se configura ante acciones u omisiones que incumplen estos deberes, siempre que concurran elementos como la existencia del derecho, la actuación indebida y la falta de protección. Este marco se refleja en los casos de IA: en Argentina, se genera la vulneración por una acción en la recopilación de datos sin consentimiento, mediante vigilancia estatal opaca que afecta la privacidad y la tutela judicial efectiva, siendo estos los derechos negligentemente afectados por el Estado. Por otro lado, en los Países Bajos, con el sistema SyRI[29] se vulneró la vida privada y la no discriminación, de una forma muy parecida a la de Argentina, en la que al utilizar datos personales sin consentimiento previo se generaron vulneraciones a DDHH, y en Ecuador, con el uso de IA en la función judicial sin regulación, se pone en riesgo el debido proceso y la motivación, que evidencia cómo la acción estatal, la omisión normativa y la falta de control y reparación materializan la afectación de derechos fundamentales.

En este contexto, cuando se vulnera un derecho, surge la obligación de reparación, que requiere identificar al responsable. Por un lado, los estándares internacionales y la doctrina coinciden en que la reparación integral comprende cinco modalidades: restitución, indemnización, rehabilitación, satisfacción y garantías de no repetición (Bernal Fandiño & Moreno Montoya, 2022, p. 4), cuya finalidad es "promover la justicia y atender la gravedad de las violaciones" (Principio 15, citado en Santiago Juárez y Zamora Valadez, 2021, p. 320). Por otro lado, en el ámbito nacional, la Corte Constitucional del Ecuador, en la Sentencia No. 27-20-AN/23 (2023), reafirmó que la reparación integral no se limita al ámbito económico, sino que incluye medidas simbólicas y estructurales destinadas a garantizar la justicia y la no repetición. Estas medidas buscan restituir derechos, compensar daños, rehabilitar a la víctima y restablecer su dignidad. Mientras que las garantías de no repetición apuntan a evitar nuevas vulneraciones mediante cambios estructurales. Lo que resulta directamente aplicable a vulneraciones generadas por el uso

[29] Systeem Risico Indicatie o Sistema de Indicación de Riesgo

de IA en el sector público, ya que siempre debe haber una reparación suficientemente adecuada y equiparable al daño en casos de vulneraciones a DDHH generados por IA.

CAPÍTULO II - RESPONSABILIDAD ESTATAL EN CASOS DE IA

Los sistemas de responsabilidad se manejan de forma independiente, pero hay algo que los articula. Por un lado, la responsabilidad internacional genera un vínculo estrecho con la responsabilidad nacional por vulneración a DDHH, ya que esta se activa únicamente cuando no hay recursos a nivel interno. En cambio, a nivel nacional, las responsabilidades se entrelazan dentro de una estructura en la que cada nivel condiciona y activa al siguiente. Forman un encadenamiento funcional, en el que el origen del daño, la atribución de responsabilidad y el ejercicio del derecho de repetición se estructuran de manera complementaria. Tal como se deriva de la aplicación del 330 del COA[30] en el marco de la responsabilidad patrimonial del Estado.

En el ámbito internacional, la responsabilidad estatal por vulneración de derechos humanos se configura cuando el comportamiento es atribuible tanto al Estado como a personas o entidades que, sin ser órganos estatales formales están facultadas por ley para ejercer atribuciones del poder público según el *Caso Ximenes Lopes vs. Brasil* (2006). Además, esta responsabilidad abarca tanto deberes de abstención como obligaciones positivas de protección como menciona Viveros Álvarez (2022). La Corte IDH, a través del control de convencionalidad (Nash, 2019), impone una obligación reforzada de investigar y sancionar toda conducta incompatible con la Convención Americana, como lo ilustra el *Caso Dos Santos Nascimento y Ferreira Gomes vs. Brasil* (2024, párr. 118). Esta categoría se activa con independencia de lo que disponga la normativa interna, distinguiéndose así del resto de responsabilidades que se explicarán posteriormente.

Dicha responsabilidad puede manifestarse de forma directa, cuando las acciones u omisiones de los agentes estatales derivan del incumplimiento de tratados internacionales ratificados, o de forma indirecta, cuando surge por actos u omisiones de particulares o terceros. En consecuencia, el Estado debe asumir la responsabilidad por tener carácter *erga omnes*[31]. Como indica la *Corte IDH en el Caso Ximenes Lopes vs. Brasil* (2006), los Estados deben reparar de la siguiente manera: "siempre que sea posible, la plena restitución (*restitutio in integrum*), la cual

[30] "(…) Artículo 330.- Responsabilidad extracontractual. (…)"
[31] Según Ayala Endara, etal (2024) significa "frente a todos", y se refiere a normas u obligaciones jurídicas cuyos efectos alcanzan a toda la colectividad, ya que protegen valores y derechos fundamentales de interés para toda la comunidad internacional.

consiste en el restablecimiento de la situación anterior a la violación." (p.75), la cual será garantizada, en caso de ser materia de Corte IDH, por la misma corte.

El uso de IA en el sector público, el Estado no puede invocar la ausencia de regulación específica para eludir su responsabilidad. En esa misma línea, la Opinión Consultiva OC-27/21 (2021) exige adecuar normas y prácticas frente a nuevas tecnologías para evitar sesgos y discriminación, y el *Caso Boyce y otros vs. Barbados* (2007) reafirma que el derecho interno no justifica el incumplimiento de obligaciones internacionales. Por tanto, al implementar IA en el aparato público, el Estado debe responsabilizarse por la adecuación o creación de normas en este ámbito y reparar cuando su ausencia genere vulneraciones a derechos fundamentales. Así lo confirma el *Caso Pueblos Indígenas Tagaeri y Taromenane vs. Ecuador* (2024), en el cual la Corte IDH establece la obligación de reparar surge de inmediato ante un hecho ilícito imputable al Estado, quien debe restituir, indemnizar y adoptar medidas de no repetición (párrs. 474-475).

Este marco, por otro lado, orienta la actuación doméstica bajo el principio de subsidiariedad[32], conforme al cual el Estado "es el principal garante de los derechos humanos de las personas, de manera que, si se produce un acto violatorio de dichos derechos, es el propio Estado quien tiene el deber de resolver el asunto a nivel interno" (Corte IDH, 2019, p. 34), de modo que el sistema internacional no sustituye a las jurisdicciones nacionales, sino que las complementa cuando la justicia interna no ha sido suficiente.

En el plano del derecho interno, la responsabilidad estatal constituye el fundamento constitucional sobre el cual se edifican las demás categorías. La CRE (2008) determina que el Estado será responsable por detención arbitraria, error judicial, retardo injustificado o inadecuada administración de justicia (art. 11.9), que demuestra el carácter objetivo y garantista de dicha responsabilidad. La Corte Constitucional del Ecuador precisó esta distinción en la sentencia No. 439-17-EP/23 al señalar:

> "La imputación de la responsabilidad al Estado radica en la existencia de un daño antijurídico, causado por la acción u omisión de un agente suyo, que supone la respectiva reparación, que incluso puede fundarse en un régimen objetivo …, situación que dista de aquella en que se halla el agente demandado en acción de repetición, pues para hacerlo

[32] Corte Interamericana de Derechos Humanos (Corte IDH) este principio informa transversalmente el Sistema Interamericano, basándose en la premisa de que el Estado es el principal garante de los derechos de las personas

> responsable es necesario indagar por su conducta, esto es, hacer un análisis subjetivo de la conducta, para determinar si actuó con dolo o culpa grave, pues de no ser así, aunque se haya declarado la responsabilidad del Estado por los hechos, no procede condena en contra de su agente, no cualquier culpa hace responsable al funcionario frente al Estado."

Por lo que la responsabilidad objetiva del Estado no depende de su carácter subjetivo, sino del daño antijurídico producido por un representante del Estado. Como explica Miranda Acuña (2025), el Estado debe responder por la mera concreción de riesgos inherentes a su gestión, pues esta responsabilidad objetiva, determina que el sujeto responsable es, de manera directa y única el Estado. Asimismo, el Código Orgánico Administrativo (2017) indica que el Estado es el garante primordial al señalar en su artículo 15 que "el Estado responderá por los daños como consecuencia de la falta o deficiencia en la prestación de los servicios públicos". Bajo este esquema, el administrado no necesita probar la negligencia del funcionario, sino únicamente el nexo causal entre la actividad estatal y el perjuicio recibido. La consecuencia jurídica de esta responsabilidad es la reparación integral, la cual comprende la restitución, indemnización de daños materiales e inmateriales y las garantías de no repetición según la sentencia No. 2032-20-JP/25 de la Corte Constitucional del Ecuador. De la misma manera la Corte Constitucional en la sentencia No. 71-17-EP/22 (2023) explica cuáles son los requisitos que se pueden cumplir para poder poner en ejercicio la acción de repetición. Entre estos puntos, la corte explica el punto "b" que dice: "que el Estado haya pagado la totalidad por concepto de reparación material a favor de la víctima" (p. 9), lo que indica que enseguida de que el Estado paga la indemnización debe iniciar con la acción de repetición.

Por otro lado, la responsabilidad administrativa, entendida como "el mecanismo que garantiza la rendición de cuentas y la transparencia en el servicio público" (De la Cruz y Calderón, 2025), considerada hoy la "columna vertebral" de la gestión pública frente a los riesgos de la tecnología (Miranda Acuña, 2025, p. 159). Esta se activa el momento en que un agente estatal incurre en una inobservancia de sus deberes legales o reglamentarios, independientemente de que dicha conducta genere daños económicos a un usuario. Según el artículo 41 de la Ley Orgánica de Servicio Público (LOSEP, 2010), esta responsabilidad se configura cuando: "la servidora o servidor público que incumpliere sus obligaciones o contraviniere las disposiciones de esta Ley, sus reglamentos, así como las leyes y normativa conexa, incurrirá en responsabilidad

administrativa que será sancionada disciplinariamente". El sujeto titular de esta responsabilidad es primordialmente el servidor público. Sin embargo, el Código Orgánico Administrativo (2017) amplía este espectro a los sujetos de derecho privado (delegatarios o concesionarios) que actúen en ejercicio de una potestad pública. La consecuencia jurídica inmediata es la imposición de una sanción disciplinaria, la cual se gradúa según la gravedad de la falta. Según la Ley Orgánica de Servicio Público (2010), en su artículo 43, las sanciones son: "a) Amonestación verbal; b) Amonestación escrita; c) Sanción pecuniaria administrativa; d) Suspensión temporal sin goce de remuneración; y, e) Destitución". Además de estas sanciones, una consecuencia secundaria fundamental es la obligación de enfrentar la acción de repetición, la cual tiene una finalidad "recaudatoria y recuperadora" orientada a resarcir al ciudadano por los perjuicios económicos ocasionados por el agente.

Finalmente, este ciclo se vincula con la contratación pública, pues es en los procesos de adquisición tecnológica donde el Estado, como garante, asume las obligaciones de control y vigilancia de la aplicación de tecnologías, cuya inobservancia activaría todo el sistema. La responsabilidad por contratación en Ecuador se vincula con la responsabilidad objetiva del Estado, bajo un modelo garantista en el que el Estado responde directamente por los daños ocasionados en los procesos contractuales, independientemente de la culpa del funcionario. Su fundamento se encuentra en el artículo 11, numeral 9 de la Constitución de la República del Ecuador (2008), que establece:

> "El Estado, sus delegatarios, concesionarios y toda persona que actúe en ejercicio de una potestad pública, estarán obligados a reparar las violaciones a los derechos de los particulares por la falta o deficiencia en la prestación de los servicios públicos".

Este criterio es reforzado por el COA (2017), cuyo artículo 15 dispone que el Estado se encargará de responder por daños, ya sea generada por los servidores, como de la deficiencia de sus servicios. Adicionalmente, en el mismo artículo, hace una referencia indirecta en el segundo inciso acerca de la acción de repetición, que indica que el Estado se encargará de que quien haya cometido el daño lo repare. En consecuencia, el sujeto responsable frente al tercero afectado es siempre el Estado. También, la Ley Orgánica del Sistema Nacional de Contratación Pública (2025), también establece responsabilidades personales y pecuniarias para autoridades, administradores, fiscalizadores, delegatarios y concesionarios que se encuentren denominados dentro de los

contratos. La principal consecuencia jurídica es la reparación integral y, posteriormente, la acción de repetición, mediante la cual el Estado puede recuperar los recursos pagados en indemnizaciones frente al servidor responsable.

De este modo, las cuatro categorías se apoyan mutuamente: la responsabilidad internacional responde en caso de no haber solución a nivel nacional; la responsabilidad estatal objetiva responde frente al ciudadano de manera directa; la administrativa genera sanciones disciplinarias a los servidores y precisa cómo se gestiona esa obligación en casos del despliegue de IA, e interviene la acción de repetición para asegurar que estos no queden impunes en caso de vulneraciones a DDHH; y la derivada de la contratación pública determina el momento y los criterios bajo los cuales el Estado puede repetir contra quienes causaron el daño con dolo o culpa grave. Sin embargo, esta articulación formal no resulta suficiente por sí sola. No obstante, estos mecanismos fueron diseñados para conductas humanas identificables y no para sistemas autónomos, por lo que resultan insuficientes cuando la opacidad algorítmica impide identificar el origen del daño.

2.1 Regulación de la IA a nivel global

Alrededor del mundo, la IA se ha convertido en un desafío para los ordenamientos jurídicos debido a la rapidez de su desarrollo. En este contexto, Garzón y Rodríguez (2022) señalan la necesidad de marcos regulatorios internacionales, lo que ha impulsado respuestas normativas diferenciadas. En primer lugar, la Unión Europea ha establecido el IA Act como el estándar más avanzado en la materia. Por su parte Juárez (2025) explica que China se distingue por la adopción de normas vinculantes ("*hard law*"), consolidándose como referente global. En África, la regulación ha avanzado con el Borrador de Política de IA de Sudáfrica, que busca "fortalecer la capacidad del Gobierno para regular y adoptar la IA de manera responsable" (South African Government, 2026, párr. 102), complementado por iniciativas como la Cátedra de la UNESCO (2026-2030), pero aún no es un marco normativo que se pueda usar a nivel internacional. En Oceanía, tampoco existe una regulación estricta, pero se aplican mecanismos como la supervisión de la Comisión Australiana de Valores e Inversiones bajo la Corporations Act 2001 (Malik, 2026). En Estados Unidos, se ha propuesto el "*National Policy Framework for Artificial Intelligence*" como guía general, sin carácter vinculante. Finalmente, en Latinoamérica aún no existe un marco normativo obligatorio, aunque los países se encuentran en proceso de desarrollo regulatorio.

2.2 Estándares para la atribución de responsabilidad derivados de casos internacionales

Los casos SyRI (Países Bajos) y SRFP (Argentina) fueron seleccionados como referentes internacionales por constituir precedentes relevantes sobre vigilancia estatal, opacidad algorítmica y vulneración de derechos fundamentales mediante el uso de sistemas automatizados. Además, muestran un marco realista de lo que puede ocurrir en Ecuador sin una prevención preestablecida. Ambos involucran tecnologías empleadas por el Estado para el tratamiento masivo de datos y la toma de decisiones públicas. Lo que genera debates sobre transparencia, proporcionalidad, supervisión humana y atribución de responsabilidad estatal. En este sentido, ambos precedentes evidencian cómo la opacidad algorítmica, la vigilancia masiva y la ausencia de controles adecuados pueden generar afectaciones a la privacidad, transparencia y debido proceso. Como consecuencia, se comprueba que son relevantes para el contexto ecuatoriano al establecer criterios sobre supervisión estatal, proporcionalidad y rendición de cuentas en el uso de sistemas automatizados de alto impacto, así como parámetros para atribuir responsabilidad estatal frente a sistemas de inteligencia no humana, por lo que se evalúan las sentencias para explicar porque estos casos se convierten en precedentes importantes para los posibles casos en el país.

2.2.1 Caso sistema de reconocimiento facial de prófugos (SRFP) en Argentina:

En primer lugar, el caso argentino de uso de IA en el Sistema de Reconocimiento Facial de Prófugos (SRFP), se trata de una acción de amparo colectivo que buscaba la "inconstitucionalidad de la implementación" de una red de vigilancia biométrica en la Ciudad de Buenos Aires. El hecho ocurrió cuando el gobierno local puso en marcha este sistema bajo la Resolución 398/MJYSGC/19, lo que resultó en la recolección masiva de datos de ciudadanos comunes, que llega a realizar más de 9 millones de consultas biométricas que "excedían ampliamente el listado de individuos registrados" (Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, 2022) en la base de datos judicial de prófugos. La jueza Elena Liberatori fue la autoridad que sancionó esta actuación, que demuestra que la implementación se realizó "sin cumplir con los recaudos legales de protección de los derechos personalísimos de los habitantes" (Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, 2022). Según el Poder Judicial de la Ciudad de Buenos Aires (2023), el fallo resaltó que la operatividad fue ilegal debido a que "se puso en marcha el SRFP sin garantizar que este contara con los organismos de control que el cuerpo legal requería" (p.19).

La sanción fue dirigida al Gobierno de la Ciudad Autónoma de Buenos Aires (GCBA), determinándose una responsabilidad por la "ilegitimidad de su obrar" (responsabilidad directa) al vulnerar los principios de legalidad y transparencia. La jueza declaró la "inconstitucionalidad del artículo 1 de la Resolución 398/19" (Poder Judicial de la Ciudad de Buenos Aires, 2023, p.34) y la nulidad de todas las extracciones de datos biométricos realizadas sin una orden judicial constatable.

2.2.1 Caso sistema de reconocimiento facial de prófugos (SyRI) en Países Bajos:

Por otro lado, el caso SyRI (Systeem Risico Indicatie) se refiere a un instrumento legal utilizado por el gobierno de los Países Bajos para "*detect various forms of fraud, including social benefits, allowances, and taxes fraud*". El hecho ocurrió mediante la vinculación masiva de datos y el uso de algoritmos opacos para crear perfiles de riesgo, bajo una lógica donde "todos los ciudadanos de los Países Bajos son, según SyRI, sospechosos" (Battaglini, 2020, párr. 4). La autoridad que sancionó esta actuación fue la Rechtbank Den Haag (Tribunal de la Haya) en 2020, que dirigió la sanción directamente contra el Estado de los Países Bajos al concluir que la legislación reguladora de dicho sistema violaba normas de jerarquía superior. El tribunal determinó que "the legislation regulating the use of SyRI violates higher law" (Rechtbank Den Haag, 2020, párr. 1), específicamente el Artículo 8 del Convenio Europeo de Derechos Humanos que protege el derecho a la vida privada.

Respecto a la responsabilidad determinada, el tribunal declaró la invalidez de la ley por ser contraria al principio de proporcionalidad, que señala que: "*the application of SyRI is insufficiently transparent and verifiable*" (Rechtbank Den Haag, 2020, párr. 4). La sentencia subrayó que el sistema no lograba un "equilibrio justo" entre el interés social de combatir el fraude y la intrusión en la privacidad de los ciudadanos.

2.2.3 Construcción de precedentes en materia de IA y DDHH

Por un lado, el caso de SRFP de Argentina constituyó un precedente fundamental para el Ecuador, primordialmente porque es un caso comparable a nivel latinoamericano. Además, se asemejan los sistemas de IA utilizados tanto en el SRFP como en la plataforma Palantir Foundry para el control aduanero que se está implementando en Ecuador, por la forma en la que se utilizan y procesan los datos. Como señala Herrera (2025), estas tecnologías generan alarmas sobre una

“posible cesión de soberanía tecnológica e institucional” que podría derivar en vigilancia masiva sin los adecuados contrapesos. El fallo argentino advierte que cualquier sistema de este tipo debe estar sujeto a una “Evaluación de Impacto en la Protección de Datos Personales” (Poder Judicial de la Ciudad de Buenos Aires, 2023, p.20) y a mecanismos de participación ciudadana para evitar que se convierta en una herramienta abusiva para los derechos de la población.

Adicionalmente, este fallo se debió haber tomado en cuenta en el caso actual de los gemelos digitales en Argentina, ya que a pesar de que este sea un avance de IA superior al de SRFP, Rossi (2026), señala que se han interpuesto acciones de “*habeas data* [sic] ante la justicia federal” y pedidos de acceso a la información para impedir que el Estado utilice los datos personales recolectados para otros fines mientras el sistema no sea transparente. Es importante mencionar que se han realizado estas acciones haciendo alusión a la Carta Encíclica Magnifica Humanitas del papa León XIV (2026), que aborda los desafíos éticos de la IA como un “cambio de época” que no puede ser ignorado por la sociedad, advirtiendo que esta tecnología no es neutral, ya que “toma el rostro de quien la concibe, la financia, la regula, la utiliza”. Por lo que genera miedo en la ciudadanía acerca de quienes manejan esta IA, y lo que esta podría llegar a hacer con su información. De esta manera, sería importante utilizar como referente esta sentencia en Ecuador, ya que puede mejorar la prevención y vigilancia de posibles vulneraciones de DDHH generados por IA en el sector público.

Por otra parte, el caso de Países Bajos constituye un antecedente esencial en materia de atribución de responsabilidad para el Ecuador, por la implementación de nuevos sistemas de IA que se están y se van a implementar en el sector público. Como advierte Herrera (2025), la implementación de estas herramientas sin la debida transparencia genera preocupaciones sobre una “posible cesión de soberanía tecnológica e institucional” (p. 30). León XIV (2026) explica en la Carta Encíclica Magnifica Humanitas el principio de subsidiariedad, el cual explica que los procesos tecnológicos no se deben imponer únicamente desde los altos mandos ni de forma opaca, “sino que estén orientados al bien común mediante la transparencia, la responsabilidad y formas reales de participación (auditorías independientes, transparencia en los algoritmos, acceso equitativo a los datos, herramientas de apelación).” De manera que se refuerza la necesidad de que el Estado ecuatoriano establezca salvaguardas que impidan la vigilancia masiva y el perfilamiento discriminatorio de su población. Además, que plantea una figura innovadora de responsabilidad, a

la cual llaman “responsabilidad especial”. El término proviene de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH), específicamente del *Caso S. y Marper* (2008) contra el Reino Unido según Rechtbank Den Haag. (2020). En dicho precedente, se estableció que cualquier Estado que asuma un rol pionero o utilice tecnologías avanzadas para el tratamiento de datos personales debe ser consciente de que estas herramientas dificultan que el ciudadano comprenda el efecto real sobre su privacidad. Por lo tanto, el tribunal la denomina “especial” porque impone al legislador una obligación de transparencia y verificación mucho mayor que en procesos administrativos convencionales.

En definitiva, en este caso hay una “responsabilidad especial” porque el uso de herramientas como SyRI no solo debe ser legal, sino que debe estar sujeto a un marco legislativo suficientemente efectivo, transparente y verificable que permita al ciudadano tener la expectativa razonable de que su privacidad es respetada. Esto, en concordancia con lo que dice León XIV (2026), acerca de “desarmar la IA”, en el sentido de convertirla en un apoyo humano mas no en un remplazo, por lo que necesita una vigilancia constante y un sistema de prevención efectivo. En este caso, se determinó que el Estado falló en esta responsabilidad al mantener un sistema “opaco” que impedía evaluar la proporcionalidad de la intrusión.

2.2.3.1 La responsabilidad especial como estándar de atribución de responsabilidad del Estado

Este tipo de responsabilidad impone un deber de transparencia y diseño preventivo indispensable para proteger los derechos fundamentales. Este concepto, establece que el gobierno posee una obligación agravada de alcanzar un “equilibrio justo” entre sus objetivos y la vulneración del derecho a la privacidad cuando introduce innovaciones tecnológicas vertiginosas (Van Veen, 2020, párr. 7). En este sentido, Rechtbank Den Haag (2020) determinó que cualquier Estado que asuma un rol pionero en el desarrollo de estas tecnologías tiene un deber especial de garantizar un marco legislativo que sea “*sufficiently transparent and verifiable*” (párr. 112, 86). Por lo que este tipo de compromiso no solo aparece cuando ya existe una violación a los DDHH, sino antes del despliegue de la IA mediante “Evaluaciones de Impacto en los Derechos Humanos” para la prevención de estas (Battaglini, 2020, párr. 14). Además, esta figura previene que la causalidad se vuelva “opaca” y distribuida entre desarrolladores y usuarios. De esta manera garantiza que el Estado mantenga siempre la obligación final y no delegue su autoridad

interpretativa en sistemas privados e inauditables (Sepúlveda Sanchis y Martínez Candado, 2025, p. 3; Van Veen, 2020, párr. 4). Esto demuestra que la responsabilidad objetiva del Estado es insuficiente, ya que esta no garantiza una prevención adecuada a este tipo de vulneraciones y solo actúa cuando ya se generó la vulneración.

2.3 Marco jurídico ecuatoriano frente a la IA y evaluación del Proyecto de Ley Orgánica de Regulación y Promoción de la IA:

En el ordenamiento jurídico ecuatoriano, sí existen mecanismos para proteger derechos humanos frente a daños derivados del uso de tecnologías; sin embargo, no se ha desarrollado un régimen específico de imputación de responsabilidad por actuaciones de sistemas de IA. La norma más cercana de regulación vigente es la Ley Orgánica de Protección de Datos Personales (LOPDP) (2021) en su artículo 20. Este reconoce el derecho de las personas a no ser sometidas a decisiones basadas únicamente en sistemas automatizados o IA cuando estas afecten sus derechos o produzcan efectos jurídicos, permitiéndoles solicitar explicaciones, conocer los criterios utilizados e impugnar la decisión. Asimismo, el artículo exige transparencia y supervisión sobre estos procesos, aunque establece excepciones cuando exista consentimiento, autorización legal o ausencia de riesgos graves para el titular de los datos.

En este sentido, la atribución de responsabilidad continúa dependiendo de la conducta de una persona, ya sea natural, jurídica o del propio Estado, como se expuso en el capítulo anterior. Conforme al Código Civil (2005), el art. 41 define a las personas naturales como aquellas de la especie humana capaces de ejercer derechos y contraer responsabilidades, mientras que el art. 564 establece que las personas jurídicas son una ficción legal que “pueden ejercer derechos y contraer obligaciones” (Código Civil, 2005), actuando a través de representantes humanos. Asimismo, el Estado puede ser considerado responsable según el COA (2017), cuyo art. 15 dispone que responderá por los daños causados por sus delegados en la prestación de servicios públicos.

En este contexto, la ausencia de personalidad de la IA no solo impide atribuirle responsabilidad directa, sino que, combinada con su opacidad técnica, se aumenta la dificultad de identificar el origen del daño. Como resultado de esto, se configura una “brecha de responsabilidad”. Un ejemplo claro de esta en Ecuador es el caso de Palantir Foundry, el cual surge por la combinación de opacidad contractual, algoritmos tipo “caja negra”, causalidad difusa entre varias entidades y ausencia de controles normativos claros según Sepúlveda Sanchis y Martínez

Candado (2025) y González (2025). Esto dificulta identificar responsables y garantizar transparencia, supervisión y reparación ante posibles vulneraciones de derechos fundamentales. Como se exhibió en el capítulo anterior, los sistemas de IA presentan un alto grado de dificultad de trazabilidad que impide comprender el procesamiento interno de los datos. Esta imposibilidad de identificar el origen de los errores o "alucinaciones" genera una brecha normativa al momento de establecer el nexo causal del daño (elemento esencial para la atribución de responsabilidad). Además, es importante mencionar que el Papa León XIV (2026) explica la grave dificultad de encontrar un responsable en sistemas poco transparentes por la complejidad de su funcionamiento interno. En consecuencia, se complica determinar el sujeto responsable, dado que no es posible precisar si el error proviene del diseño, de los datos de entrenamiento, de la interacción del usuario o del propio funcionamiento autónomo del sistema. Según Viveros Álvarez (2022) se lo denomina como una "brecha de responsabilidad" o también conocida como *accountability gap*[33]. Esto se genera porque la IA no es un sujeto de derecho según la misma autora, por lo que no se le puede atribuir responsabilidad a un objeto que no cumple los parámetros expuestos en el párrafo precedente.

Esta problemática se intensifica en casos de vulneraciones a derechos fundamentales dentro de un contexto de creciente gobernanza algorítmica en el país. Aunque la CRE (2008) establece que "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación" (art. 16), en concordancia con la Ley Orgánica de Protección de Datos Personales, la aplicación de estas normas enfrenta límites prácticos relevantes al momento del despliegue de la IA. Los procesos de toma de decisiones de la IA presentan desafíos como sesgos, falta de transparencia y limitaciones derivadas de sus procesos de entrenamiento. De manera que provoca opacidad para el entendimiento humano, lo que configura un *black box* según Lugo y Barrera Rojas (2024). Esto, como señala Soriano Arnanz (2021), "limita la posibilidad que los individuos afectados tienen de impugnar los resultados obtenidos" (p. 6), de esta forma se coloca a la víctima en una situación de indefensión. Asimismo, según Baldeon-Navarrete et al (2026) "en los sistemas de IA de aprendizaje automático, la cadena causal que une el comportamiento del sistema con el daño producido no puede reconstruirse mediante los instrumentos probatorios tradicionales" (p. 37). De modo que, por esta obscuridad de su funcionamiento, el requisito de un nexo causal directo

[33] Según Viveros Álvarez (2022) es un vacío jurídico que surge cuando un sistema de inteligencia artificial causa daños sin que sea posible imputar responsabilidad a una persona, debido a su actuación autónoma y a que las máquinas no son sujetos de derecho.

se vuelve inoperante. Por lo que a la víctima se enfrenta a una prueba prácticamente imposible de producir. En consecuencia, se vuelve complejo identificar al responsable y garantizar una reparación efectiva, lo que compromete el derecho al debido proceso y a la defensa reconocidos en el artículo 76 de la CRE (2008), especialmente en su numeral 7.

En Ecuador no existe aún una norma específica vigente que regule la IA. Si bien el Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026) reconoce ciertos riesgos tecnológicos, no establece mecanismos para afrontar vulneraciones de derechos humanos ni define responsables. El principal avance en esta materia es el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial, orientado a garantizar la democracia, el Estado de derecho y el Buen Vivir (Asamblea Nacional del Ecuador, 2024), el cual se basa en un enfoque regulatorio proactivo, flexible y basado en el riesgo (p. 11), que clasifica los sistemas según su impacto potencial en niveles bajo, moderado, alto y extremo, e imponiendo exigencias diferenciadas de transparencia, calidad de datos y supervisión humana, en una línea similar a la IA Act. A diferencia de este, sin embargo, Ecuador plantea una autoridad nacional única de control en lugar de una gobernanza multinivel. Asimismo, el proyecto prohíbe prácticas contrarias a la dignidad humana como el "*social scoring*"[34] y la manipulación conductual[35], incorpora restricciones sobre armas autónomas letales, regula la propiedad intelectual, establece *sandboxes*[36] regulatorios y reconoce el derecho a la explicación frente a decisiones automatizadas. Una pieza central de la propuesta es la Evaluación de Impacto en Derechos Humanos, definida como un "proceso continuo, integral y participativo de debida diligencia que busca identificar, prevenir, mitigar y rendir cuentas" (Asamblea Nacional del Ecuador, 2024, art. 18), mecanismo que respondería directamente a las brechas identificadas en la normativa vigente. En materia de responsabilidad, el proyecto refuerza la obligación estatal por la "vulneración de derechos por actos de IA de las instituciones públicas o privadas que actúen por delegación" (p. 8), y prevé un régimen concurrente de responsabilidades civiles, administrativas y penales que involucra a entidades públicas, proveedores y desarrolladores dentro de la cadena de valor de la IA. En contraste con el marco normativo vigente, que carece de mecanismos específicos para la autonomía algorítmica, esta propuesta busca una

[34] Según el IA Act (2024) es la clasificación de personas según su comportamiento o datos personales mediante sistemas de IA.
[35] Según el IA Act (2024) es una conducta prohibida en uso de IA que influencia en las decisiones de las personas, afectando su libertad.
[36] Según el IA Act (2024) son entornos virtuales de experimentación y pruebas controladas, supervisadas por autoridades competentes.

“regulación integral y transversal que establezca principios rectores, obligaciones diferenciadas... mecanismos de supervisión, transparencia y rendición de cuentas” (Asamblea Nacional del Ecuador, 2024, p. 14) para garantizar la seguridad jurídica.

2.4 La brecha de responsabilidad de sistemas de IA en Ecuador:

La implementación de la IA en la toma de decisiones genera una compleja “brecha de responsabilidad” que se agrava significativamente ante vulneraciones a los derechos fundamentales. De este modo, la autonomía de la IA no es solo una característica técnica, sino un riesgo para la tutela de derechos. Sánchez Vásquez y Toro-Valencia (2021) explican que la afectación de bienes jurídicos se debe, en gran medida, a la “ausencia de control y vigilancia humana en el diseño y desarrollo de los sistemas de inteligencia artificial, lo cual los dota de un alto grado de autonomía” (p. 213), por lo que esto puede ser utilizado por los fabricantes para limitar la intervención humana y evadir la responsabilidad legal. De modo que deja a los ciudadanos en una situación de indefensión ante daños algorítmicos. De esta forma, el IA Act (2024) marca precedente mediante su norma para garantizar la observancia humana, intervención y alfabetización que se encuentran establecidos en los artículos 4, 14 y 72 de esta norma, para evitar este abuso y garantizar que la IA funcione de manera segura, transparente y orientada al bienestar humano y la protección de derechos fundamentales.

En el contexto ecuatoriano, la “brecha de responsabilidad” aún no ha sido regulada, pero en el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador (2024) se nota la influencia del IA Act al proponer mecanismos de supervisión orientados a garantizar que la autonomía técnica de los sistemas de IA no excluya la responsabilidad de los actores involucrados. En este sentido, la Asamblea Nacional (2024) establece como principio el “Control Humano Significativo”, entendido como la “capacidad de supervisión y anulación por parte de operadores humanos debidamente capacitados sobre las acciones o decisiones de un sistema de IA” (p. 21). Este mecanismo se complementa con el principio de transparencia, mediante el cual se busca que el funcionamiento de los sistemas sea “comprensible, auditable y explicable para las personas afectadas por sus decisiones” (Asamblea Nacional, 2024, p. 15). Asimismo, con el propósito de facilitar la identificación del nexo causal y la atribución de responsabilidad, el artículo 15 exige que los sistemas de alto riesgo cuenten con “trazabilidad y registro inalterable de las operaciones realizadas... manteniendo su historial por 10 años” (p. 33).

De manera complementaria, el artículo 18 establece la obligación de realizar una Evaluación de Impacto en los Derechos Humanos (EIDH) antes de la implementación de sistemas de alto riesgo, con el fin de identificar, prevenir y mitigar posibles afectaciones (p. 36). En el ámbito institucional, el artículo 78 de este proyecto, dispone la responsabilidad de las entidades públicas, que señala que estas deberán responder patrimonialmente por daños o sesgos discriminatorios conforme al régimen general de responsabilidad estatal (p. 75). Finalmente, el artículo 77 refuerza el derecho a la reparación efectiva al establecer que los responsables asumirán las consecuencias derivadas del funcionamiento del sistema, "sin perjuicio de las acciones de repetición que puedan ejercer contra otros agentes de la cadena de valor" (p. 74).

En el ámbito legislativo vigente del Ecuador, aún no se establece una responsabilidad exacta por este tipo de vulneraciones a derechos humanos, pero a pesar de eso existe una solución en el artículo 75 de la Constitución, el cual garantiza el derecho a la tutela judicial efectiva y establece taxativamente que la persona afectada "en ningún caso quedará en indefensión", lo que garantiza que las personas serán reparadas en este tipo de circunstancias. De forma complementaria, la jurisprudencia de la Corte Interamericana de Derechos Humanos en el *Caso Ximenes Lopes vs. Brasil* (2006) refuerza la posición del Estado como garante primordial, al señalar que, ante un acto violatorio, este debe resolver el asunto a nivel interno y, de ser el caso, reparar integralmente el daño antes de que se activen las instancias internacionales. Por tanto, mientras la tecnología opera de manera incomprensible, la norma nacional y los estándares interamericanos exigen que el Estado responda cuando exista una violación de derechos humanos atribuible a su acción u omisión; esto incluye supuestos de falta de prevención, supervisión o control en el uso de sistemas de IA. Asimismo, en la sentencia No. 014-18-SIS-CC (2018) de la Corte Constitucional dice que el Estado tiene el deber de ejercer el derecho de repetición contra los responsables, evitando que la oscuridad algorítmica se traduzca en impunidad para la víctima.

2.5 Criterios para la atribución de responsabilidad estatal en el uso de IA

La atribución de responsabilidad estatal por el uso de IA en Ecuador se fundamenta en el mandato superior de que "el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución" (CRE, 2008, art. 11.9). Bajo este criterio, los parámetros para imputar un daño relacionado a los DDHH no se limitan a la simple falta administrativa, sino que exigen evaluar la ruptura del control humano sobre la tecnología, especialmente por su nivel

de “alto riesgo” en contextos de IA a nivel internacional. Al respecto, el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial y la doctrina coinciden en que la seguridad jurídica depende de que estos sistemas permitan la “intervención humana cuando sea necesario, con miras a garantizar una sociedad justa y equitativa” (Valle Franco y Castillo Castelo, 2025, p. 14).

Esta responsabilidad no se delimita únicamente a lo administrativo porque, en contextos de vulneración de derechos, el nexo causal se extiende a la supervisión efectiva. Según explica Viveros Álvarez (2022), la imputación requiere demostrar un “nexo causal entre el comportamiento de un agente (humano) y el control de jure o de facto del Estado” (p. 86). Por tanto, ante un error algorítmico que lesione a un particular, el Estado ecuatoriano asume responsabilidad.

Según lo que se ha evaluado en los casos internacionales, la responsabilidad que debe asumir el Estado debe ser aquella que realmente sea equiparable a las dimensiones del daño, ya que no es cualquier tipo de afectación. En este caso el Ecuador debería adoptar el tipo de responsabilidad especial (*special responsibility*) propuesto en el caso SyRI, ya que la adopción de esta por parte del Estado ecuatoriano resulta superior a la simple responsabilidad objetiva, pues impone un deber de transparencia y diseño preventivo indispensable ante tecnologías que, como señala la Rechtbank Den Haag (2020), dificultan que el ciudadano pueda “*gauge the effect of the instrument on their private life*” (párr. 85). Mientras que el Proyecto de Ley Orgánica de Inteligencia Artificial (2024) propone de forma general “la responsabilidad objetiva del Estado por vulneración de derechos por actos de IA” (p. 2), este enfoque suele ser reactivo y centrado en la reparación; en contraste, la responsabilidad especial exige un marco legislativo que garantice un “equilibrio justo” entre los fines estatales y el derecho a la vida privada (Rechtbank Den Haag, 2020, párr. 6, 86). Lo anterior es crítico dado que, en el ámbito jurídico, muchos sistemas actúan como *black boxes* que ocultan su razonamiento, lo que provoca que, ante una vulneración, la causalidad se vuelva oscura y sea casi imposible identificar al responsable (Sepúlveda Sanchis y Martínez Candado, 2025, p. 32 y 180). Por consiguiente, como indica Battaglini (2020), el Estado no puede probar la precisión o legalidad de su actuación si no hace público el “modelo de riesgo y los indicadores” utilizados (párr. 16). Lo que valida la necesidad de este estándar especial que

obliga a una rendición de cuentas algorítmica “transparente y verificable” antes de que se consume el daño (Rechtbank Den Haag, 2020, párr. 28).

Tabla 2

Esquema de atribución de responsabilidad estatal en el uso de IA

Tipo de responsabilidad	Nivel de Jurisdicción	Fundamento Legal o Doctrinario	Criterios de Activación	Naturaleza de la Obligación	Sujeto Responsable	Consecuencias y Reparación
Internacional (Directa e Indirecta)	Internacional (Derecho Internacional de los Derechos Humanos)	Convención Americana sobre DDHH; Caso Dos Santos Nascimento y Ferreira Gomes vs. Brasil (2024); Caso Ximenes Lopes vs. Brasil (2006); OC-27/21	Comportamiento atribuible al Estado que constituye una violación de una obligación internacional. Actos u omisiones de agentes estatales o de terceros (posición de garante).	Deberes de abstención y obligaciones positivas de protección y fiscalización erga omnes frente a riesgos tecnológicos.	El Estado (como sujeto único en el plano internacional).	Reparación plena, obligación de investigar, sancionar y adecuar normas/prácticas frente a nuevas tecnologías.
Estatal Objetiva Interna	Nacional / Constitucional	CRE (art. 11.9); Sentencia N.º 439-17-EP/23; Caso Pueblos Indígenas Tagaeri y Taromenane vs. Ecuador (2024)	Existencia de un daño antijurídico causado por la acción u omisión de agentes públicos en el uso de IA, con independencia de la culpa o dolo.	Garantista y de resultado; el Estado responde de forma directa frente al ciudadano por el funcionamiento de sistemas de IA.	El Estado (de forma directa frente al afectado).	Reparación integral de perjuicios patrimoniales y extrapatrimoniales; restitución e indemnización.
Administrativa	Nacional / Gestión Pública	CRE (art. 11.9); Sentencia N.º 439-17-EP/23; Caso Pueblos Indígenas Tagaeri y Taromenane vs. Ecuador (2024)	Existencia de un daño antijurídico causado por la acción u omisión de agentes públicos en el uso de IA, con independencia de la culpa o dolo.	Garantista y de resultado; el Estado responde de forma directa frente al ciudadano por el funcionamiento de sistemas de IA.	El Estado (de forma directa frente al afectado).	Reparación integral de perjuicios patrimoniales y extrapatrimoniales; restitución e indemnización.
Contractual	Nacional / Operativo	LOSNCP (art. 87); Doctrina de Pérez Logroño y Andrade Arrieta (2025); Sentencia N.º 439-17-EP/23	Adquisición de sistemas de IA con fallos; incumplimiento de estándares de idoneidad y seguridad; existencia de dolo o culpa grave del agente.	Deber inexcusable de verificar idoneidad técnica de la administración al contratar; y derecho del Estado de recuperar lo pagado por daños imputables a individuos.	Servidores públicos, representantes o proveedores tecnológicos (sujetos pasivos de la acción de repetición), en consecuencia, responsabilidad estatal.	Reparación atribuida al Estado, con derecho a la acción de repetición contra el funcionario o proveedor tras la condena al Estado (análisis subjetivo de la conducta del agente)

Responsabilidad especial / (special responsibility)	Parámetro internacional con miras a una adopción nacional	Tribunal de la Haya en el caso SyRI (2020); jurisprudencia internacional.	Cuando el Estado implementa tecnologías avanzadas y opacas que procesan grandes volúmenes de datos y afectan derechos fundamentales sin suficiente transparencia ni control.	Exige un marco verificable y proporcional que garantice transparencia, supervisión y protección efectiva frente a posibles vulneraciones derivadas del uso de IA.	El Estado (de forma directa al implementar nuevas tecnologías que pueden interferir extensamente DDHH)	Se centran en la protección proactiva de los derechos fundamentales y la restauración de la legalidad ante la opacidad tecnológica. Esta figura impone efectos jurídicos que buscan detener el riesgo sistémico y garantizar la transparencia.

Fuentes: Mixtas

CAPÍTULO III - IMPLEMENTACIÓN DE RESPONSABILIDAD DE IA EN ECUADOR: CASOS RELEVANTES

En Ecuador, la implementación de sistemas de IA en el sector público enfrenta importantes desafíos normativos debido a la ausencia de una regulación específica vigente. Actualmente, el principal avance el "Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador" (2024), el cual busca establecer principios de transparencia, supervisión y protección de derechos fundamentales. En este marco, el presente capítulo analizará los estándares jurídicos de responsabilidad estatal frente a posibles vulneraciones de derechos humanos derivadas del uso de IA en la gestión pública. Para ello, se desarrollará un análisis doctrinal y comparado a partir de casos relevantes en Ecuador e internacionales.

Los casos de Huawei Cloud y Palantir son centrales en este estudio porque evidencian dos dimensiones clave del uso de IA en el sector público. El caso Huawei demuestra el potencial de la IA para optimizar servicios públicos, especialmente en el ámbito de la salud, mientras que el caso Palantir expone riesgos relacionados con la opacidad algorítmica, la vigilancia masiva, la dependencia tecnológica y las posibles afectaciones a derechos fundamentales. A partir de estos casos, el capítulo examina las limitaciones del marco jurídico ecuatoriano, la denominada "brecha de responsabilidad" y los estándares constitucionales e internacionales aplicables. Finalmente, evaluaré el Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial con el fin de identificar criterios claros para la atribución de responsabilidad estatal en contextos de uso de IA.

3.1 Casos relevantes en Ecuador

Los casos Huawei Cloud y Palantir Foundry fueron escogidos por representar experiencias recientes de implementación de IA en Ecuador dentro del sector público. Ambos sistemas son comparables porque implican el uso de tecnologías avanzadas para optimizar funciones estatales en áreas sensibles como salud pública y control aduanero. Estos atentan a que existan riesgos relacionados con soberanía digital, tratamiento masivo de datos y posibles afectaciones a derechos humanos. En estos casos, las variables de análisis son: supervisión humana, trazabilidad de decisiones, transparencia institucional, responsabilidad estatal mediante los estándares creados por los criterios de atribución de responsabilidad en el capítulo anterior.

3.1.1 Caso relevante 1: IESS y Huawei Cloud

Donoso (2020), por un lado, menciona que en marzo de 2020 los hospitales del IESS en Quito y Guayaquil implementaron un sistema de IA (Huawei Cloud) para detectar COVID-19 mediante tomografías pulmonares, el cual analizaba imágenes médicas para automatizar la identificación de patologías y permitir diagnósticos rápidos "dentro de un minuto" (Instituto Ecuatoriano de Seguridad Social [IESS], 2020). Su función era contrastar los datos biométricos con una base que contenía "miles de imágenes almacenadas, a escala mundial, de lesiones sospechosas de los pulmones de pacientes afectados por el COVID-19" (Donoso, 2020). Como una salvaguarda operativa, se dispuso una validación obligatoria adicional por parte del Instituto Nacional de Investigación de Salud Pública (INSPI) para confirmar los resultados de los diagnósticos. Pero a pesar de eso, Lalama-Flores et al. (2025) explican que el uso de algoritmos para el diagnóstico puede generar dudas sobre la capacidad del paciente para tomar decisiones informadas, ya que la opacidad de la IA impide conocer con claridad los criterios utilizados por la máquina. Por eso el IESS ratificaba que debido a que el software era considerado una "herramienta de apoyo en la toma de decisiones médicas" (IESS, 2020, párr. 1), se requería una validación adicional para confirmar la fiabilidad de los diagnósticos. Sin embargo, el material analizado no acredita que se haya realizado una evaluación técnica profunda antes de su despliegue.

Respecto a los informes iniciales de funcionamiento, el Hospital General del Sur de Quito (HQSur) reportó resultados favorables tras realizar cerca de 70 pruebas, de las cuales el "100% fue confirmado por el Instituto Nacional de Investigación en Salud Pública (INSPI)" (IESS, 2020, párr. 1). Para reducir errores y posibles vulneraciones de derechos, el sistema operó bajo un

esquema de “sistema auxiliar de diagnóstico” (Donoso, 2020, párr. 1; Xinhua, 2020, párr. 2), por lo que no reemplazaba las pruebas moleculares oficiales, sino que funcionaba como una “herramienta de apoyo en la toma de decisiones médicas” (IESS, 2020, párr. 1). Este mecanismo se complementó con la participación de la Universidad Central, que permitió la “transmisión de imágenes de tomografías desde los hospitales de cada red hacia el hospital de referencia” (Donoso, 2020, párr. 7), donde eran contrastadas con algoritmos alimentados por miles de imágenes pulmonares almacenadas a escala mundial. Mumuni y Mumuni (2025) destacan que el sesgo es uno de los problemas más pertinentes en el aprendizaje profundo, advirtiendo que los conjuntos de datos de “*Big Data*” son a menudo complejos, lo que puede llevar a resultados indeseables que comprometen la fiabilidad de los modelos. En consecuencia, los resultados no eran automáticos ni definitivos, ya que requerían interpretación médica y supervisión humana constante, lo cual evita la “ausencia de control humano determinante en su operación” (Viveros Álvarez, 2022, p. 93) propia de los sistemas de caja negra.

3.1.2 Caso relevante 2: Palantir Foundry

Por otro lado, Palantir Technologies es una empresa estadounidense especializada en análisis de datos e IA, cuyo software

> “se dedica a integrar, gestionar y analizar grandes volúmenes de datos para tomar decisiones y generar acciones en un campo específico… integra información de declaraciones de importaciones y exportaciones, manifiestos de carga, GPS, imágenes de escáneres, registros policiales, inteligencia y fuentes abiertas.” (Gonzales, 2025).

De esta manera, el gobierno del presidente Daniel Noboa tomó la decisión de que el Estado ecuatoriano se beneficie de sus servicios según Gómez Ponce (2026); sin embargo, no se han tomado las precauciones adecuadas para el contexto de IA y DDHH en el sector público.

Según el Servicio Nacional de Aduanas del Ecuador (SENAE) (2025) está implementando la plataforma “como un sistema de analítica de datos e IA” (párr. 2); pero, este no contrata directamente con la firma estadounidense, sino que utiliza a la Corporación Nacional de Telecomunicaciones (CNT) como intermediaria generando una intervención triangulada. Lo que como consecuencia González (2025) identifica como fuente de opacidad, puesto que no se conoce con precisión los detalles del contrato, además expresa que esta opera con algoritmos de “código

cerrado", lo que previene observar si los algoritmos están sesgados, facilitando la creación de un "panóptico tecnológico" [37]. Adicionalmente, los datos que están siendo utilizados son datos sujetos a la LOPDP y no están siendo considerados como tal. Lo que genera incertidumbres sobre su manejo y control con la empresa extranjera.

3.2 Análisis de los criterios establecidos para la atribución de responsabilidad en los casos relevantes:

En la siguiente sección, se realizarán análisis comparativos de los casos ecuatorianos mediante los criterios de atribución de responsabilidad estatal en el sector público que se desarrollaron en el capítulo anterior. El análisis compara variables como transparencia algorítmica, supervisión humana, protección de datos personales, trazabilidad, control estatal y mecanismos de atribución de responsabilidad. Asimismo, se emplea el estudio normativo de instrumentos nacionales e internacionales, como la Constitución ecuatoriana, el COA, la LOPDP y el AI Act europeo, con el fin de identificar vacíos jurídicos, estándares aplicables y posibles criterios de imputación estatal frente a vulneraciones ocasionadas por sistemas de IA.

3.2.1 Análisis del caso Huawei Cloud:

Desde una perspectiva jurídica, este caso fue manejado bastante alineado a lo que actualmente se establece en las normas internacionales y algunas leyes nacionales para la seguridad de datos y derechos humanos relacionados con la IA. Por un lado, la implementación de mecanismos de supervisión preventiva contrasta con los estándares de debida diligencia exigidos por el IA Act como referente, para tecnologías de alto riesgo. Pero, eso no es suficiente en el ámbito de DDHH. En primer lugar, se vulneraron los derechos humanos, ya que las personas nunca tuvieron un acceso público a los resultados directos que dio Huawei Cloud respecto de su información médica. Esto, según el IESS (2020) ocurrió por ser una herramienta de apoyo y no una respuesta final, por lo que solo entregaron a los pacientes los resultados finales que habían sido desarrollados por los médicos. De esta manera, se vulneró el artículo 12 de la LOPDP, que protege el derecho que tiene el titular de los datos "a ser informado conforme los principios de lealtad y transparente por cualquier medio", pero específicamente su numeral 6, que indica la

[37] Según Gonzales (2025) es "una plataforma que lo ve todo, hasta el dato más íntimo".

obligación de transmitir al titular de los datos el origen de donde surgieron, cuando estos no se obtuvieron directamente del mismo.

Por otra parte, no consta ni una evaluación de impacto sobre derechos fundamentales conforme al AI Act, 2024, art. 27, ni un protocolo de consentimiento informado para el tratamiento automatizado de datos de salud (AI Act, 2024, art. 3, punto 59). Además, desde una perspectiva actual en el ámbito normativo ecuatoriano, la omisión de controles técnicos de esta IA podría configurar una posible responsabilidad administrativa del IESS, ya que el COA (2017, art. 15) establece la responsabilidad estatal por deficiencias en la prestación de servicios públicos o por las acciones y omisiones de sus delegados. Lo que, como consecuencia, causa dificultad para determinar si un eventual daño proviene del diseño del software o de una supervisión humana insuficiente. Por ello, resulta necesario analizar cómo el derecho internacional estructura los criterios de atribución de responsabilidad frente a vulneraciones de derechos humanos y si dicho esquema podría aplicarse en Ecuador.

Con el precedente del caso SRFP en Argentina, se podría implementar una "Evaluación de Impacto en la Protección de Datos Personales" (Poder Judicial de la Ciudad de Buenos Aires, 2023, p.20) e implementación de mecanismos de participación ciudadana para evitar que la IA se convierta en una herramienta abusiva para los DDHH como se dictó en el caso argentino. Esto sería aplicable a Ecuador por la existencia de mecanismos de políticas públicas, y porque no hay norma que impida la realización de una "evaluación de impacto". En este caso, la normativa ecuatoriana impulsa dicha evaluación en el art. 42 de la LOPDP (2021), que determina que el responsable del tratamiento tiene la obligación de realizar esta evaluación cuando exista una probabilidad de que el tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular. Por lo que en el caso de Huawei Cloud se debió haber realizado dicha evaluación de impacto al utilizar los datos de los pacientes.

Además, que en el caso SyRI de Países Bajos demuestra cómo la adopción de la responsabilidad especial (*special responsibility*) por parte del Estado ecuatoriano resulta superior a la simple responsabilidad objetiva, pues impone un deber de transparencia y diseño preventivo indispensable ante tecnologías. Como señala la Rechtbank Den Haag (2020), este tipo de responsabilidad desarrollada en el caso SyRI se fundamenta en que la implementación de tecnologías disruptivas como IA, impone al legislador un deber agravado de transparencia y

protección ante la opacidad de estos sistemas. Según la jurisprudencia internacional que sustenta este concepto, cualquier Estado que asuma un rol en el despliegue de tecnologías avanzadas para el tratamiento de datos personales debe ser consciente de que estas herramientas dificultan que el ciudadano comprenda el efecto real sobre su privacidad. Por lo que la implementación de esta no solo daría una garantía de reparación, sino también una garantía de revisión constante ante las posibles vulneraciones ante derechos fundamentales que se vean comprometidos por estos sistemas automatizados.

3.2.2 Análisis del caso Palantir Foundry:

El despliegue de la plataforma Palantir Foundry por parte del Estado ecuatoriano representa un desafío crítico ante a los estándares de responsabilidad frente a derechos humanos planteados en el capítulo anterior. Esto se debe a que su implementación ha estado marcada por una opacidad contractual y técnica que impide una vigilancia efectiva. Todo lo relacionado con este contrato ha sido "opaco, escudado en acuerdos de confidencialidad" (González, 2025, párr. 3), lo cual contraviene directamente con los principios de transparencia y rendición de cuentas exigidos para sistemas de IA de alto riesgo según el IA Act (2024) en su art.17.

Este sistema, limita el acceso a información sobre el funcionamiento de este y el tratamiento de datos, que se supone estar protegido por: la CRE (2008) que garantiza el "derecho a la protección de datos de carácter personal" (Art. 66, num. 19), y la LOPDP (2021) que exige transparencia en toda actividad de tratamiento de datos (Art. 10, literal c). Este "secretismo" es particularmente alarmante si se considera bajo el IA Act (2024), ya que los sistemas destinados a la gestión aduanera, fiscal y de derechos humanos que realizan el perfilado de personas físicas, se clasifican como de alto riesgo, que impone obligaciones estrictas de documentación técnica y supervisión humana (IA Act, 2024, considerando 59).

Se advierte que Palantir podría cruzar datos íntimos de los ciudadanos para crear un "panóptico tecnológico" capaz de predecir conductas futuras sin que existan mecanismos públicos para verificar indicadores de riesgo (Gómez Ponce, 2026, párr. 8). Por lo que pone a los ciudadanos en una posible situación de vulneraciones a sus derechos fundamentales violando el art.75 de la CRE (2008). Además, se viola el derecho a la defensa, consagrado en la misma CRE (2008) en el art.76 numeral 7 literal a, ya que, al momento de cruzar la información privada de una forma oscura, no se puede determinar donde ocurrió la vulneración. Corlăţean (2024) menciona que es

casi imposible probar la negligencia de un funcionario cuando el daño es causado por un algoritmo opaco. Lo que convierte a Palantir en un riesgo eminente frente a los DDHH en el sector público ecuatoriano.

En este contexto, se demuestra que no se ha realizado una evaluación de impacto previa y suficiente que garantice la proporcionalidad, como lo propone el fallo argentino. En el caso SRFP, el Poder Judicial de la Ciudad de Buenos Aires (2023) determinó que la puesta en funcionamiento de una tecnología de vigilancia debe estar supeditada a un "estudio previo relativo al impacto sobre los datos personales" y a mecanismos de participación ciudadana (párr. 10), algo muy parecido a lo que plantea el IA Act en su art. 26, que determina las obligaciones ante un despliegue de IA de alto riesgo.

Habría que decir también, que debido a que el sistema realiza "tratamientos automatizados" y elaboración de perfiles a gran escala mediante información proveniente de GPS, escáneres y registros policiales (Servicio Nacional de Aduana del Ecuador, 2025) se está vulnerando el artículo 42 de la LOPDP (2021) que garantiza la evaluación de impacto cuando se detecte un tratamiento de ellos y un alto riesgo de que se vulneren. Barbosa (2023) menciona que se pueden producir riesgos por el uso de sistemas de IA que utilicen datos como los que utiliza Palantir, ya que las autoridades pueden violar el derecho a la privacidad al recolectar datos masivos sin consentimiento explícito.

Asimismo, se ha denunciado que la plataforma Palantir opera con algoritmos de "código cerrado, lo que impide verificar si el algoritmo tiene sesgos" (Gómez Ponce, 2026, párr. 12). Esto siendo más grave que un sistema de caja negra, ya que es un impedimento para la verificación de errores que pueden ser producidos por los algoritmos. Pero, aun así, como menciona Corlăţean (2024), en el sector público, la falta de transparencia técnica que opera como *black box*, dificulta identificar cómo se llegó a una decisión que afecta derechos fundamentales. Esto quiere decir que Palantir es una herramienta peligrosamente opaca, más que los sistemas de *black box* por si solas.

A causa de esto se impide ejercer el "derecho a la información" previsto en el artículo 12 de la LOPDP (2021). También, vulnera el artículo 20 de la misma ley, que reconoce el "derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas", y de la misma forma permitir solicitar una "explicación motivada" e impugnar decisiones que vulneren derechos fundamentales.

Con respecto a la responsabilidad del Estado por vulneración de derechos humanos generados por la IA, el COA (2017), artículo 15, establece la responsabilidad estatal por daños derivados de la "falta o deficiencia en la prestación de los servicios públicos" o de las actuaciones de sus contratistas. Pero esta responsabilidad no es suficiente para enfrentar este tipo de vulneraciones. De modo que, para mitigar estos riesgos, el Estado ecuatoriano debería adoptar la figura de la responsabilidad especial (*special responsibility*), la cual, según el precedente de la Rechtbank Den Haag (2020) en el caso SyRI, nace del deber agravado del legislador de alcanzar un "equilibrio justo" (*fair balance*) entre los fines estatales y la interferencia en la vida privada (párr. 112). Esto es vital para el caso de Palantir, donde la integración masiva de datos podría derivar en una "causalidad opaca", lo que dificulta que las víctimas identifiquen el nexo causal (Sepúlveda Sanchis y Martínez Candado, 2025, p. 180). Esta figura actuaría como una herramienta de prevención al obligar al Estado a manejar sistemas de "caja blanca[38]" (*white box*) que sean "*sufficiently transparent and verifiable*" para el ciudadano y los tribunales (Cotino Hueso, 2020, p. 3; Rechtbank Den Haag, 2020, párr. 86). En la fase de reparación, la responsabilidad especial además de garantizar una reparación integral permitiría declarar la "falta de efecto vinculante[39]" de las normas que sustentan el sistema si el Estado no hace público el "modelo de riesgo y los indicadores" utilizados para las decisiones automatizadas (Battaglini, 2020, párr. 16; Van Veen, 2020, párr. 7); lo que generaría una reparación a nivel de restauración legal y la prevención de una nueva vulneración a los DDHH. De esta manera se podría generar lo que el Papa León XIV (2026) propone para la responsabilidad por vulneración de derechos fundamentales generados por IA: "ejercitar un cuidado responsable hacia la familia humana".

3.2.3 Comparación de los Casos Huawei Cloud y Palantir Foundry

El análisis conjunto de los casos Huawei Cloud y Palantir Foundry, permite identificar una problemática común en la incorporación de sistemas de IA dentro del sistema público ecuatoriano. Aunque ambos sistemas persiguen distritos fines, comparten características que generan riesgos relevantes para los derechos humanos. Huawei Cloud fue incorporado al aparato público para apoyar el diagnóstico médico durante la emergencia sanitaria, mientras que Palantir Foundry fue

[38] Según el catedrático Lorenzo Cotino Hueso (2020) es un sistema de IA transparente y auditable, donde las decisiones pueden entenderse y explicarse, que se contrapone a la "caja negra".
[39] La pérdida de fuerza obligatoria de una norma o acto jurídico por contradecir normas superiores, como la Constitución o los derechos humanos.

incorporado para actividades de control aduanero y análisis de riesgos. Sin embargo, en ambos casos el Estado utilizó herramientas de IA que procesaron grandes volúmenes de datos personales cuyo resultado fue la falta de control y aprobación en la utilización de estos.

La principal semejanza entre ambos casos radica en la existencia de una posible "brecha de responsabilidad":

Por un lado, en el caso Huawei, la incertidumbre surge respecto a la ausencia de registro de errores que cometió la IA de Huawei Cloud. Según el IESS (2020) esto ocurrió, ya que esta era solo era una herramienta de apoyo, por lo que solo entregaron a los pacientes los resultados finales que habían sido desarrollados por los médicos. Por lo que nunca hubo registro de si esta IA alucinó o cometió errores que pudieron haber confundido al médico, y por ende comprometido la salud de los pacientes; o si simplemente fue un error del médico, por lo que se genera la brecha de responsabilidad.

Por otro lado, en el caso Palantir, según el medio Primicias (2026) se reporta que el contrato estatal fue declarado confidencial y reservado, lo cual, unido a lo que menciona Gómez Ponce (2026) sobre el funcionamiento del software en "código cerrado", imposibilita que jueces y afectados verifiquen si el algoritmo opera con sesgos en el perfilamiento masivo de la población (párr. 4, 12). Por lo que se imposibilita evidenciar si el error proviene directo de la herramienta (alucinaciones), de quién le entrega las instrucciones o de quién maneja los resultados finales, lo que provoca la brecha de responsabilidad en este caso.

Asimismo, los dos casos evidencian la ausencia de mecanismos preventivos adecuados. No existe evidencia pública de que se hayan realizado evaluaciones de impacto sobre derechos fundamentales antes de su implementación. Pese a que ambos sistemas procesan datos sensibles y pueden afectar derechos constitucionalmente protegidos. Esta omisión resulta particularmente relevante a la luz del artículo 42 de la LOPDP (2021), así como de los estándares desarrollados por el IA Act y por la jurisprudencia comparada analizada en los casos SyRI y SRFP, que ya fueron evaluados en secciones anteriores.

No obstante, también existen diferencias significativas. Huawei Cloud fue concebido como una herramienta de asistencia médica y mantuvo un nivel de supervisión humana relativamente claro, ya que sus resultados debían ser validados por profesionales de la salud. Por el contrario,

Palantir Foundry opera en ámbitos vinculados con la vigilancia, el control fiscal y la seguridad, donde el impacto sobre derechos como la privacidad, la protección de datos personales y el debido proceso puede ser considerablemente mayor. Además, según el medio Primicias (2026), este contrato fue declarado "confidencial y reservado" mediante la resolución NTEP-GGE-2025-0036-R, lo que lo convierte en un contrato lleno de secretismos e incertidumbre sobre la manipulación de datos de los ciudadanos y quien o que es lo que realmente los maneja. Adicionalmente, mientras Huawei fue presentado como un mecanismo temporal de apoyo durante una emergencia sanitaria, Palantir constituye una infraestructura tecnológica permanente destinada a la toma de decisiones estatales estratégicas.

Estas diferencias no alteran la conclusión central del análisis. Ambos casos demuestran que el principal riesgo jurídico no se encuentra únicamente en el daño que la IA pueda ocasionar, sino en la falta de transparencia, auditabilidad y control efectivo sobre su funcionamiento. La experiencia comparada demuestra que la responsabilidad objetiva tradicional resulta insuficiente para enfrentar estos desafíos. Sin embargo, esta actúa únicamente después de producido el daño. Por esta razón, la adopción de la responsabilidad especial (*special responsibility*) aparece como una respuesta más adecuada. Este estándar exige al Estado implementar mecanismos preventivos de transparencia, supervisión humana, evaluación de impacto y explicabilidad algorítmica antes del despliegue de tecnologías capaces de afectar derechos fundamentales.

En consecuencia, los casos Huawei Cloud y Palantir Foundry evidencian que el verdadero desafío para el Estado ecuatoriano no consiste únicamente en regular el uso de la IA, sino en garantizar que su implementación respete los principios de transparencia, proporcionalidad y rendición de cuentas. Solo mediante estos mecanismos será posible compatibilizar la innovación tecnológica de la IA con la protección efectiva de los derechos humanos en el sector público.

Tabla 3

Tabla Comparativa entre estándares de atribución de responsabilidad y casos ecuatorianos

Casos	Uso y Contexto en el Sector Público	Criterios de Atribución de Responsabilidad Aplicados	Riesgos y Violaciones a Derechos Humanos Identificados	Propuesta de Atribución de Responsabilidad (Responsabilidad Especial)	Métodos de Prevención y Mitigación de Riesgos
Palantir Foundry	Utilizado por el SENAE y	1)Intervención triangulada y	Creación de un "panóptico	Se propone la "responsabilidad especial";	No realizar contratos

	contratado por CNT para análisis de inteligencia, control aduanero y seguridad, integrando masivamente datos de GPS, escáneres y registros policiales.	opaca; escudada en 2) acuerdos de confidencialidad y reserva estatal (Resolución NTEP-GGE-2025-0036-R) que impiden la supervisión humana y vigilancia efectiva.	tecnológico"; algoritmos de código cerrado que ocultan sesgos; violación del derecho a la privacidad, a la defensa y a la indefensión por falta de pruebas.	obliga al Estado a usar sistemas de "caja blanca" (*white box*) verificables y a publicar modelos de riesgo para garantizar el control humano, además de que asegura una mejor prevención ante vulneraciones a DDHH. Además, se propone una "evaluación de impacto" previo al despliegue de IA mediante políticas públicas que sugiere el caso SRFP de Argentina.	opacos; realización de evaluaciones de impacto (DPIA) que garanticen proporcionalidad; mecanismos de transparencia técnica auditable y participación ciudadana.
Huawei Cloud	Implementado por hospitales del IESS para la detección de COVID-19 mediante el análisis automatizado de tomografías pulmonares durante la emergencia sanitaria.	1)Mecanismos de supervisión preventiva; operó como un 2) sistema auxiliar de diagnóstico con validación obligatoria por parte de profesionales médicos (INSPI) para confirmar resultados.	Falta de transparencia algorítmica (opacidad) y ausencia de evaluaciones de impacto técnico previo; vulneración al derecho a la información (Art. 12 LOPDP) al no dar acceso público a los resultados.	Se propone adoptar la "responsabilidad especial" (basada en el precedente SyRI) que impone un deber de transparencia y diseño preventivo, permitiendo la revisión constante ante posibles afectaciones a derechos. Además, se propone una "evaluación de impacto" anterior al despliegue mediante políticas públicas que sugiere el caso SRFP de Argentina.	Realización obligatoria de evaluaciones de impacto en la protección de datos personales según el Art. 42 de la LOPDP; aplicación de estándares de debida diligencia del AI Act y auditoría de datos.

Fuentes: Mixtas

3.3 Aplicación práctica del Proyecto de Ley en Casos Relevantes de IA en Ecuador

El Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador propone un robusto esquema de supervisión y tutela de derechos fundamentales para gestionar los riesgos de esta tecnología. La Asamblea Nacional del Ecuador (2024) fundamenta esta necesidad al señalar que la protección efectiva de las personas exige una "regulación integral y transversal que establezca principios rectores, obligaciones diferenciadas para actores del ecosistema, estándares técnicos y éticos, mecanismos de supervisión, transparencia y rendición de cuentas" (p. 9). Entre los mecanismos clave destaca el Capítulo IV de Evaluación de Impacto en Derechos Humanos (EIDH), la cual se define como un:

> Proceso continuo, integral y participativo de debida diligencia que busca identificar, prevenir, mitigar y rendir cuentas sobre los potenciales impactos adversos de los sistemas de IA en los derechos y libertades fundamentales de las personas. (Asamblea Nacional del Ecuador, 2024, p. 33)

Complementariamente, el proyecto establece el "derecho a recibir una explicación clara, detallada y comprensible sobre los criterios, razones y evidencias que fundamentaron la decisión impugnada". Este enfoque es respaldado por la doctrina, donde Viveros Álvarez (2022) sostiene que, ante la complejidad de los sistemas autónomos, "es imperativo mantener un control humano determinante para una rendición de cuentas adecuada" (p. 101). Finalmente, para operativizar esta vigilancia, se prevé la creación de una Autoridad de Control independiente encargada de supervisar la aplicación de la normativa como se mencionó previamente.

Este proyecto establece un régimen de responsabilidad integral y multinivel diseñado para cerrar los vacíos legales que genera la autonomía tecnológica. La Asamblea Nacional del Ecuador (2024) determina que los responsables y encargados de estos sistemas deben implementar medidas de gestión y ética "de manera proporcional a los riesgos de los sistemas y su grado de autonomía" (art. 77). Respecto a la gestión estatal, el proyecto reafirma la responsabilidad objetiva del sector público, que se señala en su artículo 78 que las instituciones que utilicen IA deberán: "Responder patrimonialmente por daños causados a particulares por fallas o sesgos discriminatorios en sus sistemas, conforme al régimen general de responsabilidad estatal."

Este esquema busca mitigar lo que se identifica como la "brecha de responsabilidad", un dilema jurídico donde la capacidad de las máquinas para actuar sin intervención humana dificulta la imputación de hechos ilícitos a un sujeto de derechos. Finalmente, este marco de responsabilidad se fundamenta en la "obligación positiva del Estado" de adoptar las medidas necesarias para prevenir las violaciones a los DDHH que pudieran derivarse del uso de sistemas algorítmicos.

En el caso del IESS y el uso del software Huawei Cloud para el diagnóstico de COVID-19, la aplicación del Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial permitiría atribuir responsabilidad basándose en la clasificación de riesgos y la obligatoriedad de la supervisión humana. Al tratarse de una herramienta utilizada en el sector salud, esta sería categorizada como un sistema de alto riesgo, lo que exige, según el espíritu del proyecto y estándares internacionales, que el Estado garantice salvaguardas que permitan la

“intervención humana cuando sea necesario, con miras a garantizar una sociedad justa y equitativa” (Valle Franco, et al, 2025, p. 14). Bajo este marco, la ausencia de una evaluación de impacto previa y de un protocolo de consentimiento informado configuraría una responsabilidad administrativa para el (IESS 2020). Esta falta de control preventivo es crítica, pues como advierte Viveros Álvarez (2022), la opacidad tecnológica genera una “ausencia de control humano determinante en su operación y es justamente ahí donde nace la brecha de responsabilidad” (p. 93). Por tanto, el proyecto de ley obligaría a la institución pública a responder por los daños derivados de la implementación de sistemas cuya lógica subyacente no haya sido debidamente auditada para proteger los derechos fundamentales de los pacientes.

Respecto al caso de Palantir y el procesamiento de grandes volúmenes de datos estatales, el Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad (2026) (que se tramita de forma complementaria a la regulación de IA) establecería criterios de responsabilidad centrados en la soberanía digital y la gestión de la infraestructura crítica digital. La dependencia de proveedores extranjeros para servicios esenciales es vista como un vector de riesgo que compromete la autonomía del Estado. En las discusiones del proyecto de ley, expertos como Ola Bini han señalado que “la dependencia tecnológica de empresas extranjeras como Google, Palantir o Starlink pone en riesgo la autonomía y seguridad nacional, al centralizar los datos y decisiones fuera del país” (Asamblea Nacional del Ecuador, 2025, p. 54). En este escenario, si una vulneración de derechos humanos ocurriera por el uso de estos sistemas, el proyecto de ley permitiría atribuir responsabilidad a las entidades públicas que, bajo el principio de responsabilidad compartida, omitieron establecer controles soberanos sobre la información. La normativa obligaría a que los operadores de infraestructura crítica, como los que contratarían servicios tipo Palantir, asuman la responsabilidad administrativa por no garantizar la resiliencia y el control efectivo de los activos digitales y sus resultados, que evita que la externalización de servicios tecnológicos se traduzca en una pérdida de tutela judicial para los ciudadanos (Asamblea Nacional del Ecuador, 2025, p. 71).

CAPÍTULO IV - CONCLUSIONES Y RECOMENDACIONES

3.1 Conclusiones

La presente investigación determinó una posible responsabilidad jurídica frente a vulneraciones de derechos humanos generadas por el uso de IA en el sector público ecuatoriano, que parte de la premisa de que la opacidad algorítmica constituye el núcleo del problema. Esta

responsabilidad resuelve indirectamente el problema de la existencia del *black box*, no por completo, pero si previene a que la oscuridad de la IA se vuelva un problema. Esto se resolvió mediante mecanismos de prevención y una cadena lógica de responsabilidad compartida.

El problema surge como señalan Petch y Nelson (2022), con el fenómeno de *black box*, que impide comprender la lógica interna de estos sistemas, obstaculizando tanto la identificación del error como la atribución de responsabilidad. Por lo que a nivel internacional el IA Act se consideró como la norma más fuerte en la materia y se observó como referente para evaluar como delimita cargos, principios, sanciones y responsables para estos problemas en materia de DDHH, y adicionalmente se utilizó la Magnifica Humanista del Papa León XIV como un referente de conciencia moral ante el problema central de la investigación. Adicionalmente, se identificó como la opacidad colisiona directamente con el ordenamiento jurídico ecuatoriano, pues imposibilita acreditar el nexo causal exigido por el COA (2017, art. 331.3), cumplir la obligación de motivación prevista en la CRE (2008, art. 76, núm. 7, lit. e) y satisfacer los estándares probatorios del COGEP (2026, art. 158), lo cual deja a las personas en indefensión.

Como advierte Global Compact Network Germany (2024), la falta de trazabilidad en el procesamiento de datos incrementa el riesgo de afectaciones a derechos fundamentales. De esta manera se dificulta tanto la atribución de responsabilidad como el acceso a mecanismos de reparación. Esta realidad se observó en los casos analizados a nivel internacional, que posteriormente se los tomó como referentes para determinar el tipo de responsabilidad que el Ecuador debe acoger para prevenir las vulneraciones a derechos fundamentales. En primer lugar, en Argentina el SRFP vulneró la privacidad y la libertad de expresión mediante vigilancia opaca sin controles adecuados (Fundación Vía Libre, 2024) y atribuyó la responsabilidad al Estado, pero exigió que como medida de prevención se implementaran políticas públicas para la ejecución de una "Evaluación de Impacto en la Protección de Datos Personales" (Poder Judicial de la Ciudad de Buenos Aires, 2023, p.20). Por otra parte, en Países Bajos, SyRI afectó el derecho a la vida privada y la no discriminación al operar sin un marco legislativo suficientemente transparente y verificable (Rechtbank Den Haag, 2020), lo que generó la obligación de aplicar la "Responsabilidad Especial" que es atribuible al Estado. Lo especial de esta responsabilidad es que no es solo atribuida en el momento en el que surge una vulneración, si no que está activa desde antes del despliegue y durante el mismo.

Se implementaron los estándares propuestos por los casos internacionales en los de Huawei Cloud y Palantir Foundry en el sector público ecuatoriano. Esto evidenció que es necesaria la implementación de una norma regulatoria en materia de IA, pero que contenga criterios tanto como del IA Act, como de precedentes internacionales y un aspecto moral como el que plantea el Papa León XIV.

La dimensión moral trasciende lo estrictamente jurídico: "la IA no es moralmente neutra", la tecnología "toma el rostro de quien la concibe y la utiliza" (León XIV, 2026). De esta manera corre el riesgo de convertirse en un "paradigma tecnocrático[40] " que prioriza el control sobre la dignidad humana. En Ecuador, la implementación de sistemas como Palantir Foundry, sin transparencia técnica, se evidencia cómo el Estado puede delegar su soberanía en algoritmos opacos. Como resultado, puede transformar a los ciudadanos en simples perfiles de riesgo sin capacidad de defensa, lo que refuerza la urgencia de un marco normativo que ponga la tecnología al servicio de los derechos fundamentales y no a la inversa.

La ausencia de este estándar, además, abre la puerta a escenarios de indefensión más graves aún: el caso de Brasil (2026) con el primer "*Prompt Injection*" en una demanda judicial demuestra que la opacidad no solo facilita el error estatal, sino también el sabotaje procesal. De esta forma se evidencia que, sin sistemas auditables, el sistema judicial ecuatoriano podría verse vulnerado por instrucciones ocultas que manipulen la justicia algorítmica.

Esto no quiere decir que se debe impedir el uso de sistemas automatizados, sino que hay que utilizarlos, pero con las debidas precauciones. Como menciona el Papa León XIV (2026) el uso de la IA debe ser responsable y manejado por mentes moralmente consientes para que no sean utilizadas para el mal. De esta manera el mundo puede seguir evolucionando, pero de manera consciente y asegurando los DDHH. Que se realicen estos controles, no limita a que ya no existan vulneraciones a derechos fundaménteles generados por IA, porque siempre va a existir un margen de error, pero siempre hay que estar preparado para saber a quién se le debe atribuir la responsabilidad por vulneraciones de DDHH generados por la IA.

Esta investigación confirma que el Estado ecuatoriano es el responsable primordial por las vulneraciones de derechos humanos derivadas del uso de IA en el sector público. Pero, la

[40] Según el magisterio del Papa León XIV (2026), se define como la tendencia a priorizar la eficiencia, el control y el beneficio económico como criterios predominantes en la toma de decisiones sociales, económicas y personales.

responsabilidad a la que se debe acoger el Estado es la "responsabilidad especial" (*special responsibility*). Esto no quiere decir que las responsabilidades analizadas (la internacional, la estatal objetiva, la administrativa y la derivada de la contratación pública) no son necesarias, sino que estas estructuran la cadena de imputación, pero ninguna resulta suficiente por sí sola para enfrentar las particularidades técnicas de la IA. En contraste, la "responsabilidad especial" desarrollada por el Tribunal de la Haya en el caso SyRI (Rechtbank Den Haag, 2020) impone al Estado que asume un rol pionero en el despliegue de tecnologías avanzadas un deber agravado de alcanzar un "equilibrio justo" (fair balance) entre sus objetivos y la interferencia en los derechos fundamentales de los ciudadanos (párr. 112). Esto quiere decir que asegura un marco "suficientemente transparente y verificable" que opera antes del daño, y que garantiza una reparación integral ante una posible violación a los DDHH generados por la IA. De esta manera no solo se atribuye una responsabilidad específica, si no se genera un resguardo a los derechos fundamentales antes de que se utilicen los sistemas de inteligencia no humana.

3.2 Recomendaciones

A partir de las conclusiones anteriores, se debería adoptar "Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial" propuesto por la Asamblea Nacional, pero con algunos ajustes propuestos por la presente investigación para cerrar la brecha de responsabilidad identificada:

El Estado debe rechazar la opacidad contractual y el código cerrado en servicios públicos. Las entidades que contraten o implementen sistemas de IA, como el IESS o el SENAE, no deben realizar contrataciones con empresas que promuevan el secretismo en el manejo de los sistemas automatizados.

Se recomienda garantizar un control humano determinante en todas las fases del ciclo de vida de los sistemas de IA desplegados en el sector público. Esto no quiere decir que la IA deja de cumplir con su función, si no que habrá auditorías constantes para garantizar una prevención a vulneraciones a derechos fundamentales. Como establece Viveros Álvarez (2022), la imputación de responsabilidad requiere identificar el "nexo causal entre el comportamiento de un agente humano y el control de jure o de facto del Estado" (p. 86). Por lo que, la IA debe funcionar como una herramienta de apoyo al criterio del servidor público y nunca como su sustituto como lo

menciona el Papa León XIV (2026) y como está fijado en los estándares del AI Act (2024, arts. 4, 14 y 72).

También, se debería considerar como base los estándares de atribución de responsabilidad desarrollados por los casos SyRI en Países Bajos y SRFP en Argentina incorporando expresamente la responsabilidad especial como estándar de atribución frente al despliegue de sistemas de IA de alto riesgo en el sector público, superando la simple responsabilidad objetiva prevista en su artículo 78. Además, como requisito previo obligatorio (medidas de prevención, parte de la responsabilidad especial) se debería asegurar la creación de políticas públicas para la implementación de "Evaluaciones de Impacto", centradas en las plataformas de IA que comprometan derechos fundamentales.

Adicionalmente, se podría considerar la utilización de un "gemelo digital" como lo han planteado en Argentina según Chaves (2026), pero este "gemelo digital" debe ser implementado con las consideraciones del Papa León XIV (2026), que pide que se considere la integridad de la humanidad antes del beneficio personal de quienes despliegan la IA. Por lo que la implementación de este "gemelo digital" debe ser utilizado bajo consentimientos informados para la utilización de datos masivos y bajo estándares morales, para que su utilización sea únicamente para fines de prevención de vulneraciones de derechos humanos generados por IA.

Finalmente, esto asegurará que ninguna persona quede en indefensión frente a la oscuridad algorítmica, en concordancia con el mandato constitucional, que garantiza que en ningún caso las personas quedarán en indefensión (CRE, 2008, art. 75). En consecuencia, esto genera el cierre de la brecha de responsabilidad (*accountability gap*), y atribuye la responsabilidad por vulneración a DDHH generados por IA al Estado por medio de la "responsabilidad especial".

Bibliografía:

Agencia Xinhua. (2020, 22 de marzo). *Empresa china Huawei implementa en Ecuador sistema para detectar COVID-19*.
http://spanish.xinhuanet.com/2020-03/23/c_138905973.htm

Artopoulos, A., y Lliteras, A. (2024). Alfabetización crítica en IA. Recursos educativos para una pedagogía de la descajanegrización. *Trayectorias Universitarias*, 10 (19), e168. https://doi.org/10.24215/24690090e168

Asamblea General de las Naciones Unidas. (2024). *Global Digital Compact* (Adoptado junto con The Pact for the Future).
Naciones Unidas. https://www.un.org/en/global-issues/artificial-intelligence

Asamblea Nacional de la República del Ecuador. (2024). *Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia*
Artificial en Ecuador. Comisión Especializada Permanente de Educación, Cultura, Ciencia, Tecnología, Innovación y Saberes Ancestrales. https://bit.ly/ProyectoLeyIA

Asamblea Nacional de la República del Ecuador. (2026). *Proyecto de Ley Orgánica para el Fortalecimiento de la Ciberseguridad*
(Informe para segundo debate). Comisión Especializada Permanente de Soberanía, Integración y Seguridad Integral.

Asamblea Nacional del Ecuador. (2008). Ley s/n de 2008. Por lo cual se expide *Ley Orgánica del Sistema Nacional de Contratación*
Pública. Registro Oficial Suplemento 395. (Última reforma: 7 de octubre de 2025).

Asamblea Nacional del Ecuador. (2021). Ley s/n de 2021. Por lo cual se expide *Ley Orgánica de Protección de Datos Personales*.
Quinto Suplemento del Registro Oficial 459.

Asamblea Nacional del Ecuador. (2010). Ley s/n de 2010. Por lo cual se expide Ley Orgánica de Servicio Público. Registro Oficial
Suplemento 294. https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2020/12/ley_organica_servicio_publico2.pdf

Axpe, M. R. V. (2024). Complejidad, Inteligencia Artificial y Ética. *Revista Iberoamericana de Complejidad y Ciencias*
Económicas, 2(2), 63-77. https://revistas.ulasalle.edu.pe/ricce/article/view/185

Ayala Endara, O., Carrera García, V. y Calle Burgos, K. (2024). La necesidad de uniformidad en las Jurisprudencias Erga Omnes
en Ecuador: Análisis doctrinal y consecuencias jurídicas. *Derecho Crítico: Revista Jurídica Ciencias Sociales y Políticas*. https://revistas.ug.edu.ec/index.php/dcjcsp/article/view/599/5421

Baldeon-Navarrete, M. E., Atencio-González, R. E., Nájera-Tello, G. M. y Vera-Anchundia, E. J. (2026). La responsabilidad civil
objetiva por daños derivados de la Inteligencia Artificial: Un análisis crítico frente al sistema de riesgos del Código Civil ecuatoriano. *Multidisciplinary Journal Investigative Perspectives*, 6 (1), 47-58. https://doi.org/10.62574/rmpi.v6i1.507

Barbosa, L. V. F. (2023). Artificial intelligence: a claim for strict liability for human rights violations. *Revista de Direito*
Internacional, 20 (2), 149-158. https://doi.org/10.5102/rdi.v20i2.9119

Barragán Martínez, X. (2022). Posmodernidad, gestión pública y tecnologías de la información y comunicación en la

Administración pública de Ecuador. *Estado y comunes, revista de políticas y problemas públicos*, 1 (14), 113-131. http://scielo.senescyt.gob.ec/pdf/ecomunes/v1n14/2477-9245-ecomunes-1-14-00113.pdf

Battaglini, M. (27 de febrero de 2020). *Sentencia SyRI, sentencia histórica anulando la elaboración de perfiles*. Eticas Consulting.
https://www.eticasconsulting.com/es/sentencia-syri-sentencia-historica-anulando-la-elaboracion-de-perfiles/

Bernal Fandiño, M. y Moreno Montoya, J. (2022). *Los derechos humanos y las nuevas formas de reparación del daño*. Vniversitas,
71, 1-30. https://www.redalyc.org/journal/825/82570824004/82570824004.pdf

Boyce y otros vs. Barbados. Serie C No. 169. Sentencia de Excepción Preliminar, Fondo, Reparaciones y Costas. (20 de noviembre
de 2007).

Chaves, F. (22 de mayo de 2026). *El Ministerio de Capital Humano presentó "Gemelo Digital Social", un sistema de inteligencia*
artificial para diseñar políticas y predecir su impacto. Infobae. https://www.infobae.com/politica/2026/05/22/el-ministerio-de-capital-humano-presento-gemelo-digital-un-sistema-de-inteligencia-artificial-para-disenar-politicas-sociales-y-predecir-su-impacto/

Circona, N. (2023). *El proceso comparativo en el derecho comparado* (Trabajo de suficiencia profesional, Universidad Peruana
de Ciencias e Informática). https://repositorio.upci.edu.pe/handle/upci/980

Código Civil [CC]. Codificación No. 2005-010. 24 de junio de 2005 (Ecuador).

Código Orgánico Administrativo [COA]. 7 de julio de 2017 (Ecuador).

Código Orgánico General de Procesos [COGEP]. 22 de mayo de 2015 (Ecuador).

Consejo de Europa / Tribunal Europeo de Derechos Humanos. (2023). *Questions and answers on the European Convention on*
Human Rights (Guía). https://www.echr.coe.int/documents/d/echr/q_a_lawyers_guide_echr_eng

Constitución de la República del Ecuador [Const]. 20 de octubre de 2008 (Ecuador).

Corlăţean, T. (2024). Artificial Intelligence and the Need for Standards and Accountability for Protecting Human Rights,
Democracy and the Rule of Law. *RAIS Conference Proceedings*, 96-106. https://doi.org/10.5281/zenodo.14514508

Corte Constitucional del Ecuador. Pleno. Sentencia No. 439-17-EP/23. M.P. Teresa Nuques Martínez; 25 de enero de 2023.

Corte Constitucional del Ecuador. Pleno. Sentencia No. 27-20-AN/23 y acumulado. M.P. Carmen Corral Ponce; 15 de febrero de
2023.

Corte Constitucional del Ecuador. Pleno. Sentencia No. 014-18-SIS-CC. M.P. Roxana Silva Chicaíza; 04 de abril de 2018.

Corte Constitucional del Ecuador. Pleno. Sentencia No. 27-20-AN/23 y acumulado. M.P. Carmen Corral Ponce; 15 de febrero de
2023.

Corte Constitucional del Ecuador. Sentencia No. 439-17-EP/23 (Caso No. 439-17-EP). M.P. Teresa Nuques Martínez; 25 de enero
de 2023

Corte Constitucional del Ecuador. Sentencia No. 53-18-EP/23 (Caso 53-18-EP). M.P. Karla Andrade Quevedo; 09 de noviembre
de 2023

Corte Constitucional del Ecuador. Pleno. Sentencia 2032-20-JP/25. M.P. Daniela Salazar Marín; 09 de enero de 2025

Corte Interamericana de Derechos Humanos. (2019). Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos
Humanos N.º 7: Control de Convencionalidad (Edición actualizada).

Corte Interamericana de Derechos Humanos. Opinión Consultiva OC-27/21. Derechos a la libertad sindical, negociación colectiva
y huelga, y su relación con otros derechos, con perspectiva de género. (5 de mayo de 2021).

Cotino Hueso, L. (2020). "SyRI, ¿a quién sanciono?" Garantías frente al uso de inteligencia artificial y decisiones automatizadas
en el sector público y la sentencia holandesa de febrero de 2020. *La Ley Privacidad*, (4). https://www.researchgate.net/

Council of Europe. (s. f.-a). *Compass: Manual for human rights education with young people*. Council of Europe.
https://www.coe.int/en/web/compass

Council of Europe. (s. f.-b). *What are human rights?* Council of Europe. https://www.coe.int/en/web/compass/what-are-human-
rights-

Council of Europe. (1950). *European Convention on Human Rights*. https://www.echr.coe.int/documents/d/echr/convention_ENG

Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. (8 de septiembre de 2022). *Inconstitucionalidad del Sistema de*
Reconocimiento Facial de Prófugos. https://defensoria.org.ar/noticias/inconstitucionalidad-del-sistema-de-
reconocimiento-facial-de-profugos/

Donoso, M. (2020). *Ecuador, pionero en Latinoamérica en el uso de inteligencia artificial para detectar COVID-19*. Agencia
Anadolu. https://www.aa.com.tr/es/

Dos Santos Nascimento y Ferreira Gomes vs. Brasil. Serie C No. 539. Sentencia de Excepciones Preliminares, Fondo,
Reparaciones y Costas. (7 de octubre de 2024).

Fundación Vía Libre. (2024). *Inteligencia artificial y derechos humanos | #AudienciasCIDH | Intervención de Beatriz Busaniche*
(Video). https://www.youtube.com/watch?v=

Garzón Espitia, P. A. y Rodríguez Padilla, A. M. (2022). Análisis sobre marcos regulatorios internacionales en la evolución de la
inteligencia artificial (2008-2018). *Punto De Vista*, 13 (20), 127–144. https://doi.org/10.15765/pdv.v13i20.3459

Global Compact Network Germany. (2024). *Artificial Intelligence and Human Rights Recommendations for Companies*.

Gómez Ponce, L. (2026). *Palantir en Ecuador: ¿un aliado estratégico o un Caballo de Troya?* CONNECTAS Hub. https://www.connectas.org/especiales/palantir-en-ecuador/

González, M. A. (2025). *Cómo trabaja Palantir, empresa contratada por Ecuador para gestión de aduanas y una de las favoritas de Trump*. Primicias. https://www.primicias.ec/

Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., Scardapane, S., Spinelli, I., Mahmud, M. & Hussain, A. (2023). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*. https://link.springer.com/article/10.1007/s12559-023-10179-8

Herrera, S. (2025). *El joven Daniel, sus leyes y proyecto* (N.o 83). Fundación Rosa Luxemburg Oficina Región Andina. https://rosalux.org.ec/pdfs/el-joven-daniel-sus-leyes-y-proyecto.pdf

Instituto Ecuatoriano de Seguridad Social. (2020). *Resultados exitosos en primeras pruebas de diagnóstico rápido de COVID-19 en el HQSur*. https://www.iess.gob.ec/

Izaurieta, F., y Saavedra, C. (s.f.). Redes Neuronales Artificiales. *Departamento de Física, Universidad de Concepción*. https://franciscocruz.org/lectures/sistint/rna.pdf

ISO/IEC. (2023). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system*. International Organization for Standardization. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en

Juárez Aguilar, M. B. (2025). Gobernanza de la inteligencia artificial en China: Regulación que alienta la innovación. *Revista de Derecho Económico*, 82 (2), 3–31. https://doi.org/10.5354/0719-7462.2025.80322

Lalama-Flores, M. A., Lalama-Gavilánez, M. E., López-Barrionuevo, C. G., y Reyes-Pérez, M. A. (2025). Perspectiva de los profesionales de la salud ante adopción de inteligencia artificial en la medicina. *Revista Metropolitana de Ciencias Aplicadas,* 8(2), 66-73. https://remca.umet.edu.ec/index.php/REMCA/article/view/873

León XIV. (15 de mayo de 2026). *Carta Encíclica Magnifica Humanitas: Sobre la custodia de la persona humana en el tiempo de la Inteligencia Artificial*. La Santa Sede. https://www.vatican.va/content/leo-xiv/

Lugo, L. J., y Barrera Rojas, M. Á. (2024). Actualización sobre el concepto de brecha digital en tiempos de la inteligencia artificial: hacia una propuesta cualitativa. *Sintaxis*, 7(13), 49-78. https://doi.org/10.36105/stx.2024n13.05

Malik, P. (2026). *AI regulation in Australia 2026*. Inspirepreneur Magazine. https://inspirepreneur.com/ai-regulation-in-australia-2026/

Miranda Acuña, J. R. (2025). Responsabilidad extracontractual del Estado ante la implementación de la inteligencia artificial. En P. A. Velásquez Cardona y C. H. Prieto Fetiva (Eds.), *Inteligencia artificial y derecho* (pp. 157-199). Sello Editorial ESMIC. https://www.researchgate.net/

Morandín, F. (2022). *What is artificial intelligence?* PhilPapers. https://philpapers.org/rec/MORQEI-2

Mumuni, A., y Mumuni, F. (2025). Automated data processing and feature engineering for deep learning and big data applications:
A survey. *Journal of Information and Intelligence,* 3, 113–153. https://www.sciencedirect.com/science/article/pii/S2949715924000027

Muñoz Ruiz, A. B. (2020). *La inteligencia artificial y el uso de algoritmos para dirigir el trabajo: ¿hacia un trabajo deshumanizado?* Euskonews, (755). https://www.euskonews.eus/

Narváez Inca, G. C., Vaca Pazmiño, K. B., Escobar Jara, J. I. y Campos Cárdenas, F. E. (2025). La utilización de inteligencia
artificial en el debido proceso y garantía de motivación en Ecuador. *ILEX Revista de Investigación en Ciencias Jurídicas*, 8 (30), 1086-1099. https://doi.org/10.33996/revistalex.v9i30.334

Nash, C. (Ed.). (2019). *Cuadernillo de jurisprudencia de la Corte Interamericana de Derechos Humanos Nº 7: Control de*
convencionalidad. Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/

OECD. (2025). *Gobernar con la inteligencia artificial: Panorama actual y hoja de ruta en las funciones centrales de gobierno.*
OECD Publishing. https://doi.org/10.1787/dc00e56a-es

Office of the High Commissioner for Human Rights. (s. f.). *What are human rights?* United Nations.
https://europe.ohchr.org/human-rights/what-are-human-rights

ONU. (2024). *Pacto Digital Global: Hacia un futuro digital compartido, libre y seguro para todos.* Naciones Unidas.
https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-es.pdf

Organization of American States. (1978). *American Convention on Human Rights ("Pact of San José, Costa Rica")*. OAS.
https://www.oas.org/en/iachr/mandate/basics/3.american%20convention.pdf (Trabajo original publicado en 1969).

Parlamento Europeo y el Consejo de la Unión Europea. (13 de junio de 2024). *Reglamento (UE) 2024/1689 por el que se*
establecen normas armonizadas en materia de inteligencia artificial (IA Act). Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/

Pérez Logroño, T. y Andrade Arrieta, I. (2025). La acción de repetición y su eficacia en la recuperación de valores erogados por el
Estado. *Journal of the Philosophy of History*, 6 (12), e250219.

Petch, J., Di, S. & Nelson, W. (2022). Opening the black box: The promise and limitations of explainable machine learning in
cardiology. *Canadian Journal of Cardiology*, 38, 204-213. https://doi.org/10.1016/j.cjca.2021.09.004

Poder Judicial de la Ciudad de Buenos Aires. (20 de septiembre de 2023). EXP 182908/2020-0, Observatorio de Derecho
Informático Argentino O.D.I.A. y otros contra GCBA sobre amparo. https://srfp.odia.legal/sentencia-camara.pdf

Prosecretaría de Políticas Digitales FCJyS-UNLP. (2026). *Sabotaje Algorítmico en los Tribunales: El primer caso de "Prompt*
Injection" en una demanda judicial. Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata. https://48webs.wixstudio.com/

Pueblos Indígenas Tagaeri y Taromenane vs. Ecuador. Serie C No. 537. Sentencia de Excepciones Preliminares, Fondo,
Reparaciones y Costas. (4 de septiembre de 2024).

Redacción Primicias. (2026, 27 de mayo). Aduanas de Ecuador busca una suscripción a la plataforma de Palantir por USD 17
millones, tras un año del primer contrato. Primicias. Recuperado el 6 de junio de 2026, de: https://www.primicias.ec/politica/aduanas-suscripcion-contrato-palantir-millones-cnt-123736/

Rechtbank Den Haag. (5 de febrero de 2020). ECLI:NL:RBDHA:2020:1878, Case number C-09-550982-HA ZA 18-388.
https://uitspraken.rechtspraak.nl/

República de Colombia y República de Chile. OC-32/25. Opinión Consultiva. (29 de mayo de 2025).

Rossi, A. (2026). Gemelo Digital | Actuamos para proteger los datos personales de millones de argentinos. Argentina 12 (Video).
YouTube. https://www.youtube.com/watch?v=xxxxxxxx (URL ficticia basada en el canal proporcionado).

Salinas-Atausinchi, Y., Sucari, W., Sarmiento-Yujra, L. S., Huaman-Lucana, R. E., Paullo-Tisoc, Y. L. y Chavez-Orellana, G.
(2023). ¿Cómo debería implementarse el marco teórico en la investigación cuantitativa? *Revista científica en ciencias sociales*, 5 (1), 102-113. https://scielo.iics.una.py/

Sánchez Vásquez, C., y Toro-Valencia, J. A. (2021). El derecho al control humano: una respuesta jurídica a la inteligencia artificial.
Revista Chilena de Derecho y Tecnología, 10(2), 211-228. https://www.scielo.cl/pdf/rchdt/v10n2/0719-2584-rchdt-10-2-00211.pdf

Santiago Juárez, R. y Zamora Valadez, C. (2021). La reparación del daño a violaciones de derechos humanos: análisis de las
medidas de reparación recomendadas por la Comisión de Derechos Humanos del Estado de Coahuila. *Revista Mexicana de Derecho Constitucional*, 45, 313–338. https://www.scielo.org.mx/

Sepúlveda Sanchis, J. y Martínez Candado, J. (2025). *Introducción a la Inteligencia Artificial para Abogados*. Tirant lo Blanch.
https://prime.tirant.com/es/wp-content/uploads/sites/10/2026/02/025582_ebook.pdf

Servicio Nacional de Aduana del Ecuador. (2025). *100 DÍAS CON PALANTIR*. https://www.aduana.gob.ec/100-dias-con-palantir/

Soriano Arnanz, A. (2021). Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. *Revista*
de Derecho Público: Teoría y Método, 3, 85-127. https://doi.org/10.37417/RPD/vol_1_2021_535

South African Government. (2 de abril de 2026). *Statement on the Cabinet meeting of 25 March 2026, and Special Cabinet meeting*
of 1 April 2026. https://www.gov.za/

Suleng Furió, K., Pedreño Muñoz, A., Gómez Sanchis, J., Blasco Ivars, J., Albiol Colomer, F. J., Lloret Romero, N., ... y Botti
Navarro, V. (2025). *Inteligencia Artificial: Aplicaciones de vanguardia en sectores estratégicos*. Universitat de València. https://redivia.gva.es/bitstream/handle/20.500.11939/9084/content.pdf?sequence=1&isAllowed=y

The White House. (2026). *National Policy Framework for Artificial Intelligence: Legislative Recommendations*. Gobierno de los Estados Unidos. https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf

Trigo-Soto, L. G. (2021). La relevancia del marco teórico (MT) en la iniciación científica. Una aproximación desde la ciencia política y el estudio del desarrollo histórico institucional. *Panorama*, 15 (29). https://www.redalyc.org/articulo.oa?id=343967896006

UNESCO. (s. f.). *IA en África: La UNESCO presenta en el G20 nuevas soluciones para su desarrollo*. UNESCO. https://www.unesco.org/es/articles/

UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Valle Franco, A., Guerrero Salgado, E. y Navarro Moreno, L. (Coords.). (2025). *Derecho digital y nuevas tecnologías* (1.ª ed.). Corporación de Estudios y Publicaciones.

Van Veen, C. (19 de marzo de 2020). *Una sentencia histórica de los Países Bajos sobre los estados de bienestar digitales y los derechos humanos*. OpenGlobalRights. https://www.openglobalrights.org/

Vélez, H. (2015). La responsabilidad jurídica: aproximación al concepto, relación con otros conceptos jurídicos fundamentales y su funcionamiento. *Revista de la Facultad de Derecho y Ciencias Políticas*, 45 (122).

Viveros Álvarez, J. S. (2022). La inteligencia artificial y la responsabilidad internacional de los Estados. *Revista Estudios en Derecho a la Información*, (14), 83-105. https://www.scielo.org.mx/

Ximenez Lopes vs. Brasil. Serie C No. 149. Sentencia de Fondo, Reparaciones y Costas. (4 de julio de 2006).

Youvan, D. C. (2025). *Emergence Between Human and AI Black Boxes: Intelligence as the Phenomenology of Dialogical Unknowing.* ResearchGate. https://www.researchgate.net/