

DERECHOS **HUMANOS**

frente a la automatización
de las decisiones públicas

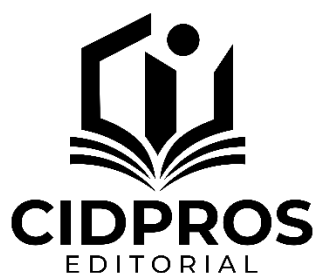


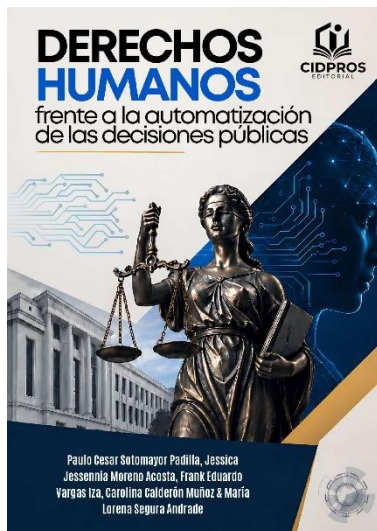
**Paulo Cesar Sotomayor Padilla, Jessica
Jessennia Moreno Acosta, Frank Eduardo
Vargas Iza, Carolina Calderón Muñoz & María
Lorena Segura Andrade**



Derechos humanos frente a la automatización de las decisiones públicas

Paulo Cesar Sotomayor Padilla, Jessica Jessennia
Moreno Acosta, Frank Eduardo Vargas Iza, Adriana
Carolina Calderon Muñoz & María Lorena Segura
Andrade





Datos bibliográficos

ISBN	978-9907-9574-9-5
Título del libro	Derechos humanos frente a la automatización de las decisiones públicas
Autores	Paulo Cesar Sotomayor Padilla Jessica Jessennia Moreno Acosta Frank Eduardo Vargas Iza Adriana Carolina Calderon Muñoz María Lorena Segura Andrade
Editorial	CIDPROS EDITORIAL
Materia	340 - Derecho
Público objetivo	Profesional / académico
Año	2026
Número de edición	1
Tamaño	3,34Mb
Soporte	Libro digital descargable
Formato	PDF (.pdf)
Idioma	Español
DOI	https://doi.org/10.67166/a42jey15

Hecho en Ecuador / Made in Ecuador

MSc. Paulo Cesar Sotomayor Padilla

Investigador Independiente

asesor.paulo@gmail.com

<https://orcid.org/0009-0000-7736-082X>

Babahoyo, Los Rios, Ecuador

Semblanza

Paulo Cesar Sotomayor Padilla, destacado ingeniero en Contabilidad y Auditoría originario de Ecuador, se desempeña actualmente como Auditor Externo calificado por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria. Su sólida formación académica incluye maestrías en Contabilidad y Finanzas en la Universidad Católica De Santiago De Guayaquil, así como en Contabilidad y Auditoría en Mención en Gestión Tributaria por la Universidad Espíritu Santo, y una maestría en Derecho Tributario por la Universidad ECOTEC; actualmente, se encuentra cursando un Doctorado (PhD) en Administración de Empresas en la Universidad Central de Querétaro.



Con una amplia trayectoria en consultoría y capacitación, su ejercicio profesional se orienta bajo principios de rigor técnico y actualización constante en áreas de cumplimiento y normativa legal. Entre sus contribuciones académicas destaca su investigación sobre jurisprudencia e inteligencia artificial en la responsabilidad jurídica, publicada en revistas indexadas de prestigio. El Magíster Sotomayor se distingue por su compromiso ético y su capacidad analítica, cualidades que emplea para fortalecer la transparencia financiera y la seguridad jurídica en las instituciones, aportando significativamente al desarrollo del sistema empresarial y tributario de la sociedad ecuatoriana.

MSc. Jessica Jessennia Moreno Acosta

Universidad Estatal de Milagro
jessica.moreno47@gmail.com
<https://orcid.org/0009-0003-1776-8403>
Milagro, Guayas, Ecuador

Semblanza

Jessica Jessennia Moreno Acosta es una psicóloga ecuatoriana nacida el 12 de julio de 1990 en Milagro, provincia del Guayas, un entorno donde consolidó un profundo compromiso social y una firme vocación de servicio orientada a brindar una atención psicológica oportuna, eficiente y profundamente humana. Desde el inicio de su carrera desarrolló una alta sensibilidad hacia las realidades de los sectores más vulnerables, lo que ha guiado su trayectoria hacia la defensa de la equidad, la inclusión y el bienestar integral de la comunidad.



Cuenta con una sólida formación académica: es Psicóloga de profesión y obtuvo el título de Máster en Intervención Psicosocial, encontrándose actualmente cursando una segunda maestría en Psicología Clínica con mención en Psicoterapia. Su preparación se respalda con múltiples certificaciones especializadas en psicología educativa, neuropsicología, estrategias de regulación emocional, así como en Diseño Universal para el Aprendizaje (DUA). Esta constante capacitación refleja su búsqueda de la excelencia científica y su actualización permanente para responder con rigor y calidez a las necesidades únicas de sus pacientes.

A lo largo de su trayectoria, ha destacado tanto en la práctica institucional como en el ejercicio libre, colaborando activamente en la Cruz Roja en el apoyo a jóvenes y adultos mayores, y desempeñándose como facilitadora en el Ministerio de Inclusión Económica y Social (MIES) brindando atención psicológica domiciliaria a personas con discapacidad. Actualmente, ejerce sus servicios en el ámbito municipal y en su consultorio privado, priorizando la atención a grupos de atención prioritaria y niños con dificultades de aprendizaje. Su vocación académica e investigadora se evidencia en la publicación de artículos científicos y en la coautoría de otros libros; en esta nueva obra, aporta una visión humanista indispensable sobre la defensa de los derechos humanos frente a la automatización de las decisiones públicas, encarnando valores de resiliencia, ética e integridad al servicio de la transformación social.

MSc. Frank Eduardo Vargas Iza

Investigador Independiente

ab.frankvargas@gmail.com

<https://orcid.org/0009-0004-8463-4859>

Puyo, Pastaza, Ecuador.

Semblanza

Frank Eduardo Vargas Iza es un abogado ecuatoriano originario de la región amazónica, con una sólida formación académica orientada al ámbito jurídico y de los derechos humanos. Posee una maestría en Derechos Humanos y Sistemas de Protección por la Universidad Internacional de La Rioja, además de diplomados en liderazgo y en derechos de los pueblos indígenas dentro del sistema interamericano. Actualmente se encuentra cursando el último semestre de un doctorado en Derecho Internacional, lo que evidencia su constante interés por la especialización y el crecimiento académico.



En el campo profesional, ha desarrollado una trayectoria relevante en el sector público, académico y social. Se ha desempeñado como asesor jurídico en el Ministerio de Agricultura y Ganadería, donde participó en procesos legales vinculados a organizaciones sociales y resolución de conflictos. Asimismo, ha trabajado en la Universidad Estatal Amazónica en áreas académicas y jurídicas, fortaleciendo su experiencia en normativa institucional. En la actualidad, dirige una fundación enfocada en la defensa de los derechos de comunidades indígenas, liderando acciones estratégicas y de representación legal.

Su perfil se distingue por un fuerte compromiso con los derechos humanos, la justicia intercultural y la resolución de conflictos desde un enfoque integral. Es autor de un artículo científico sobre contratos electrónicos en Ecuador, donde analiza sus desafíos legales en el contexto actual. Además, cuenta con habilidades en argumentación jurídica, mediación y litigación, y domina tanto el inglés como el kichwa, lo que le permite una conexión directa con comunidades indígenas y una práctica profesional orientada a la equidad, la inclusión y el respeto a la diversidad cultural.

Abg. Carolina Calderón Muñoz

Investigador Independiente

ab.carolinacalderonm@gmail.com

<https://orcid.org/0009-0005-8229-8908>

Playas, Guayas, Ecuador

Semblanza

Carolina Calderón Muñoz es una jurista ecuatoriana, con más de 10 años de experiencia en el ámbito público y privado, desde muy temprana edad fortaleció su sensibilidad social y conciencia ambiental, que pudo desarrollar utilizando al Derecho como una herramienta al servicio de su país, desarrollándose en múltiples instituciones como Consejo Nacional de la Judicatura, Universidad de Guayaquil, Federación Nacional de Cooperativas Pesqueras, Cooperativas de transportes y otras.

Cuenta con una sólida formación académica: es abogada, magister en relaciones internacionales con mención en cooperación Internacional, Magister en Derecho Constitucional, Doctora Honoris Causa como reconocimiento a su trayectoria Social, Experta en Derechos Humanos con enfoque en Género, diplomada en Políticas Públicas, actualmente se desempeña como abogada litigante, y conferencista internacional en Derecho Ambiental y sustentabilidad, en diversas Universidades de Latinoamérica demostrando así su compromiso con la Academia y el medio ambiente siguiendo los lineamientos de los Objetivos del desarrollo sostenible.

Convencida de que solo una comunidad instruida, puede hacer cambios significativos, escribe artículos que contribuyan a investigadores y al desarrollo de futuros profesionales.



Abg. María Lorena Segura Andrade

Investigador Independiente

malorenasegura@gmail.com

<https://orcid.org/0009-0004-8960-3904>

Quito, Pichincha, Ecuador

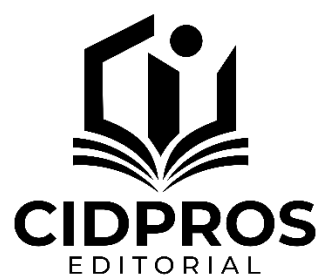
Semblanza

María Lorena Segura Andrade es abogada con más de quince años de experiencia en el sector público, con una trayectoria profesional enfocada principalmente en derecho administrativo, patrocinio institucional, régimen disciplinario, servicio público y gestión jurídica del talento humano. A lo largo de su carrera ha ejercido funciones de asesoría y representación institucional, sustanciación de procedimientos administrativos, elaboración de criterios jurídicos y aplicación de normativa vinculada con la administración pública y la gestión del talento humano.



En cuanto a su formación profesional es Abogada de los Juzgados y Tribunales del Ecuador por la Pontificia Universidad Católica del Ecuador y Máster en Gestión Ambiental, Calidad y Auditoría para Empresas por EUDE Business School, Madrid. Además, es mediadora certificada por el Colegio de Abogados de Pichincha y egresada de la carrera de Psicología de la Universidad Técnica del Norte. Esta formación multidisciplinaria complementa su ejercicio jurídico con herramientas vinculadas al análisis organizacional, la gestión de conflictos y el fortalecimiento de las relaciones laborales e institucionales.

Actualmente desarrolla su actividad profesional en el Gobierno Autónomo Descentralizado del Distrito Metropolitano de Quito, dentro de la gestión jurídica de talento humano, donde ha asumido funciones de coordinación, supervisión de procesos, patrocinio institucional y asesoramiento jurídico. Su trayectoria refleja una orientación permanente hacia el servicio público, el rigor técnico, la defensa institucional y la aplicación del Derecho como instrumento para fortalecer una gestión pública responsable, transparente y respetuosa de los derechos y garantías de las personas.



El contenido y las ideas expuestas en esta obra se encuentran protegidos por la normativa vigente en materia de propiedad intelectual y constituyen derechos exclusivos de su(s) autor(es).

Todos los derechos reservados © 2026

Sinopsis

Esta obra examina los principales desafíos jurídicos que surgen cuando la administración pública incorpora inteligencia artificial, algoritmos y sistemas automatizados en sus procedimientos y decisiones. El análisis parte de la transformación digital del sector público y aborda los límites que deben observarse cuando la tecnología interviene en actuaciones capaces de afectar derechos, obligaciones e intereses legítimos. Se estudian especialmente la igualdad y la no discriminación algorítmica, la privacidad, la protección de datos personales, la transparencia, la explicabilidad y la motivación de las decisiones automatizadas. Asimismo, se analizan las garantías vinculadas con el debido proceso, la intervención humana, la impugnación, el control administrativo y judicial, la determinación de responsabilidades y los mecanismos de reparación. Desde una perspectiva centrada en los derechos humanos, la obra sostiene que la eficiencia tecnológica debe mantenerse subordinada a principios de juridicidad, proporcionalidad, transparencia, supervisión y rendición de cuentas. El objetivo es ofrecer una visión integral de las condiciones jurídicas necesarias para que la automatización pública contribuya a mejorar la gestión estatal sin reducir las garantías que protegen a las personas frente al ejercicio del poder público.

Palabras clave: automatización pública; derechos humanos; inteligencia artificial; protección de datos; transparencia algorítmica.

Synopsis

This book examines the main legal challenges that arise when public administration incorporates artificial intelligence, algorithms, and automated systems into its procedures and decision-making processes. The analysis begins with the digital transformation of the public sector and addresses the limits that must be observed when technology intervenes in actions capable of affecting rights, obligations, and legitimate interests. Particular attention is given to equality and algorithmic non-discrimination, privacy, personal data protection, transparency, explainability, and the reasoning of automated decisions. The book also examines guarantees related to due process, human intervention, the right to challenge decisions, administrative and judicial oversight, the determination of responsibility, and mechanisms for remedy and restitution. From a human-rights-centered perspective, the book argues that technological efficiency must remain subordinate to legality, proportionality, transparency, supervision, and accountability. Its purpose is to provide an integrated legal framework for understanding the conditions under which public-sector automation can improve institutional performance without weakening the guarantees that protect individuals against the exercise of public authority.

Keywords: public-sector automation; human rights; artificial intelligence; data protection; algorithmic transparency.

Índice de Contenido

Sinopsis	10
Synopsis	11
Introducción	14
Capítulo 1 Automatización y transformación de la administración pública	17
1.1 Transformación digital de la administración pública	18
1.2 Concepto y características de la automatización administrativa	21
1.3 Inteligencia artificial y sistemas algorítmicos en la gestión pública	25
1.4 Ámbitos de aplicación de las decisiones automatizadas en el sector público	28
1.5 Eficiencia administrativa y límites de la automatización	31
1.6 Riesgos de la delegación de decisiones públicas a sistemas automatizados	34
1.7 Derechos humanos como límite y criterio de la transformación digital pública	38
Capítulo 2 Igualdad y no discriminación algorítmica	42
2.1 Principio de igualdad y prohibición de discriminación en la actuación pública	43
2.2 Concepto y manifestaciones de la discriminación algorítmica	46
2.3 Sesgos en los datos utilizados por sistemas automatizados	49
2.4 Sesgos en el diseño y funcionamiento de los algoritmos	52
2.5 Impacto diferenciado de las decisiones automatizadas en grupos vulnerables	55
2.6 Discriminación directa, indirecta y algorítmica	59
2.7 Evaluación y prevención de impactos discriminatorios	62
2.8 Obligaciones de la administración pública frente a la igualdad algorítmica	65
Capítulo 3 Privacidad y protección de datos personales	69
3.1 Privacidad y protección de datos como derechos fundamentales	70
3.2 Tratamiento de datos personales por sistemas automatizados públicos	73
3.3 Recolección, integración y reutilización de datos en la administración pública	76
3.4 Perfilamiento ciudadano y elaboración automatizada de perfiles	79
3.5 Datos sensibles y riesgos derivados de su procesamiento automatizado	82

3.6 Principios de protección de datos aplicables a la automatización pública.....	86
3.7 Límites jurídicos al uso de datos personales en decisiones automatizadas.....	89
Capítulo 4 Transparencia y explicación de decisiones automatizadas	93
4.1 Transparencia administrativa en entornos de automatización	94
4.2 Opacidad algorítmica y dificultades para comprender la decisión pública	97
4.3 Derecho a conocer el uso de sistemas automatizados.....	99
4.4 Explicabilidad de algoritmos y decisiones administrativas	103
4.5 Motivación de los actos administrativos automatizados.....	106
4.6 Acceso a la información sobre datos, criterios y procedimientos utilizados	109
4.7 Transparencia algorítmica como condición para el control ciudadano y jurídico	113
Capítulo 5 Garantías jurídicas y reparación de derechos vulnerados	117
5.1 Debido proceso frente a decisiones públicas automatizadas.....	118
5.2 Derecho a la intervención y revisión humana	121
5.3 Derecho de impugnación de decisiones automatizadas	124
5.4 Control administrativo y judicial de los sistemas algorítmicos	127
5.5 Determinación de responsabilidad por decisiones automatizadas	131
5.6 Prueba del daño y de la vulneración de derechos en entornos algorítmicos.....	134
5.7 Mecanismos de reparación y restitución de derechos vulnerados	137
5.8 Garantías institucionales para una automatización pública compatible con los derechos humanos	140
Conclusión	144
Bibliografía	147

Introducción

La incorporación de sistemas automatizados e inteligencia artificial en la administración pública está modificando de manera profunda la forma en que las instituciones procesan información, organizan procedimientos y adoptan decisiones. Estas tecnologías permiten analizar grandes volúmenes de datos, clasificar solicitudes, establecer prioridades, detectar patrones y apoyar actuaciones que anteriormente dependían exclusivamente de la intervención humana. Sin embargo, la transformación tecnológica del Estado no constituye únicamente un proceso de modernización administrativa. También plantea interrogantes jurídicos relacionados con la forma en que deben protegerse los derechos de las personas cuando una decisión pública es producida, condicionada o recomendada mediante sistemas algorítmicos.

La automatización ofrece posibilidades importantes para mejorar la eficiencia, rapidez y capacidad operativa de las instituciones públicas. Procesos repetitivos pueden desarrollarse en menor tiempo, determinadas inconsistencias pueden identificarse automáticamente y las entidades pueden disponer de herramientas adicionales para organizar grandes cantidades de información. No obstante, estas ventajas deben evaluarse junto con los riesgos que aparecen cuando los sistemas tecnológicos intervienen en decisiones capaces de producir efectos jurídicos. La eficiencia administrativa no puede convertirse en un criterio absoluto que permita reducir garantías, limitar mecanismos de defensa o trasladar decisiones sensibles a herramientas cuyo funcionamiento no pueda ser suficientemente comprendido, supervisado o controlado.

Uno de los principales desafíos consiste en determinar hasta qué punto puede delegarse la actividad decisoria de la administración. Los sistemas automatizados pueden asumir funciones muy diferentes: algunos se limitan a organizar información, mientras otros clasifican personas, generan puntuaciones, establecen niveles de riesgo o formulan recomendaciones con considerable influencia sobre la decisión final. Esta diversidad obliga a distinguir entre automatización auxiliar, automatización parcial y decisiones con mayor grado de autonomía tecnológica. Cuanto mayor sea la influencia del sistema sobre derechos, prestaciones, sanciones o cargas, mayor deberá ser también la intensidad de las garantías jurídicas, la supervisión humana y los mecanismos institucionales de revisión.

La igualdad y la prohibición de discriminación ocupan un lugar central dentro de esta problemática. Los algoritmos no operan en un vacío social, sino a partir de datos, variables, criterios y objetivos establecidos durante su diseño e implementación. Por ello, pueden

reproducir desigualdades existentes, utilizar variables indirectamente asociadas con condiciones protegidas o generar tasas de error diferentes entre determinados grupos. El riesgo aumenta cuando las decisiones automatizadas afectan a personas en situación de vulnerabilidad o cuando las consecuencias negativas se reproducen sistemáticamente. La evaluación de estos sistemas debe considerar tanto su funcionamiento técnico como los resultados concretos que producen sobre distintas personas y colectivos.

La privacidad y la protección de datos personales representan otra dimensión fundamental de la automatización pública. Los sistemas algorítmicos dependen frecuentemente de grandes cantidades de información para identificar patrones, elaborar perfiles, realizar inferencias o producir recomendaciones. Esta capacidad puede mejorar determinados procesos administrativos, pero también aumentar las posibilidades de recopilación excesiva, reutilización incompatible, interconexión de registros o utilización de información sensible. El hecho de que una institución disponga técnicamente de determinados datos no significa que pueda utilizarlos sin límites. Todo tratamiento debe responder a finalidades legítimas, criterios de necesidad y proporcionalidad, condiciones de seguridad y garantías que permitan mantener control sobre la información personal.

La transparencia constituye igualmente una condición indispensable para una administración automatizada compatible con los derechos humanos. Cuando un sistema tecnológico interviene en una decisión pública, la persona debe poder conocer que dicha intervención ocurrió y comprender cuál fue su función dentro del procedimiento. La transparencia no puede reducirse a informar que se utilizó inteligencia artificial. Debe proporcionar elementos que permitan identificar los datos relevantes, los principales criterios de valoración, el grado de intervención humana y la relación entre el resultado tecnológico y la decisión administrativa. Sin esta información, resulta difícil detectar errores, cuestionar resultados o determinar responsabilidades.

La explicabilidad se encuentra estrechamente vinculada con esta exigencia de transparencia. Una decisión pública debe poder traducirse a razones comprensibles para la persona afectada, incluso cuando su elaboración haya incluido modelos complejos. La dificultad técnica de un algoritmo no puede justificar que la administración comunique únicamente una puntuación, clasificación o resultado final sin explicar su significado. La motivación jurídica continúa siendo responsabilidad de la autoridad pública. Por ello, la automatización debe diseñarse y utilizarse de manera que los resultados puedan relacionarse con los hechos del caso, los criterios aplicados y las normas que fundamentan la actuación administrativa.

El debido proceso es esencial cuando las decisiones automatizadas afectan derechos u obligaciones. Las personas deben poder conocer la actuación, formular observaciones, corregir datos, cuestionar criterios y solicitar revisión. La intervención humana debe ser efectiva y no meramente formal. El funcionario responsable necesita información, competencia y autonomía para evaluar el resultado algorítmico, considerar las particularidades del caso y modificar la decisión cuando existan razones jurídicas o fácticas que lo justifiquen.

La posibilidad de impugnar las decisiones automatizadas conduce directamente al problema del control administrativo y judicial. Los sistemas utilizados por la administración deben mantener niveles suficientes de trazabilidad que permitan reconstruir qué información se empleó, qué procedimiento se siguió y quién intervino en la decisión. La auditoría, las evaluaciones de impacto, los registros de funcionamiento y los mecanismos de revisión permiten detectar errores individuales y problemas estructurales. Cuando estas garantías resultan insuficientes, el control judicial debe permanecer disponible para examinar la legalidad de la actuación, proteger derechos y ordenar las medidas necesarias para corregir las consecuencias derivadas de un uso inadecuado de sistemas automatizados.

La responsabilidad y la reparación completan este marco de protección. La utilización de algoritmos no puede producir espacios en los que resulte imposible determinar quién responde por una decisión perjudicial. La institución pública continúa siendo responsable de las tecnologías que selecciona, contrata, configura y utiliza dentro del ejercicio de sus competencias. Cuando una decisión automatizada vulnera derechos, la respuesta jurídica debe dirigirse no solo a corregir el resultado individual, sino también a identificar las causas que lo produjeron. Dependiendo del caso, pueden ser necesarias medidas de restitución, rectificación de datos, revisión de perfiles, modificación del sistema, compensación o garantías destinadas a evitar que la vulneración vuelva a repetirse.

Esta obra analiza la automatización pública desde los derechos humanos, abordando transformación digital, igualdad, no discriminación, privacidad, protección de datos, transparencia y explicación de decisiones. También examina las garantías de revisión, responsabilidad y reparación frente a posibles vulneraciones. Su propósito es establecer condiciones jurídicas para un uso legítimo de la tecnología, promoviendo una administración pública eficiente, transparente, controlable, responsable y compatible con la protección efectiva de los derechos de las personas.

Capítulo **1**

Automatización y transformación de la administración pública

Paulo Cesar Sotomayor Padilla



1.1 Transformación digital de la administración pública

La transformación digital de la administración pública comprende un proceso de cambio institucional en el que las tecnologías digitales modifican procedimientos, servicios, estructuras organizativas y formas de relación entre el Estado y la ciudadanía. No se limita a sustituir documentos físicos por registros electrónicos, ya que implica reorganizar la producción, circulación y utilización de información dentro de las entidades públicas. Van Noordt y Misuraca (2022) explican que la incorporación de inteligencia artificial en el gobierno puede entenderse como una modalidad de innovación pública apoyada por tecnologías de información y comunicación. Su adopción, sin embargo, exige considerar las características organizativas propias del sector público.

La digitalización administrativa ha avanzado desde sistemas destinados principalmente a registrar y procesar información hacia herramientas capaces de apoyar análisis, clasificaciones, predicciones y decisiones. Zuiderwijk et al. (2021) identifican que la inteligencia artificial aplicada a la gobernanza pública presenta implicaciones relacionadas con la prestación de servicios, la toma de decisiones y la organización institucional. En este contexto, la transformación digital modifica la forma en que la administración obtiene y procesa datos para cumplir sus competencias. El cambio tecnológico, por tanto, incide directamente en la capacidad administrativa, pero también plantea interrogantes sobre la manera en que deben conservarse las garantías propias de la actuación pública.

En Ecuador, esta transformación debe desarrollarse dentro de los principios constitucionales que regulan la administración pública. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 227, la administración pública constituye un servicio a la colectividad y debe regirse por principios como eficacia, eficiencia, calidad, coordinación, participación, planificación, transparencia y evaluación. La incorporación de herramientas digitales puede contribuir al cumplimiento de varios de estos principios, pero su utilización no modifica la finalidad jurídica de la actividad administrativa. Una plataforma automatizada sigue siendo un medio empleado por una institución pública para cumplir competencias cuya legitimidad deriva del ordenamiento jurídico.

Esta sujeción jurídica resulta relevante porque la innovación tecnológica no concede a la administración un ámbito autónomo de actuación. El Código Orgánico Administrativo (2017), en su artículo 14, establece el principio de juridicidad y dispone que la actuación administrativa se somete a la Constitución, los instrumentos internacionales, la ley, los principios y la

jurisprudencia aplicable. En consecuencia, cualquier proceso de transformación digital debe integrarse dentro de ese marco normativo. Un sistema informático puede modificar la velocidad o la forma mediante la cual se procesa una solicitud, pero no puede alterar por sí mismo las competencias legales, eliminar garantías procedimentales ni establecer condiciones carentes de fundamento jurídico.

La incorporación de inteligencia artificial también modifica las capacidades internas de las organizaciones públicas. Neumann et al. (2024) estudian la adopción de estas tecnologías en organizaciones públicas y muestran que su incorporación depende de factores organizacionales y contextuales que exceden la disponibilidad técnica de una herramienta. Esto obliga a considerar competencias del personal, recursos, liderazgo, infraestructura, coordinación y adaptación de procesos. La transformación digital requiere, por tanto, decisiones institucionales sobre dónde y para qué emplear sistemas automatizados. Una administración puede disponer de tecnologías avanzadas y, al mismo tiempo, carecer de procedimientos adecuados para integrarlas de manera coherente con las responsabilidades que corresponden a sus servidores públicos.

En los gobiernos locales, la adopción de inteligencia artificial presenta condiciones similares. Yigitcanlar et al. (2024), al revisar experiencias de implementación en administraciones locales, destacan que la incorporación efectiva de estas tecnologías depende de factores institucionales y de prácticas concretas de adopción. Esto permite diferenciar transformación digital de simple adquisición tecnológica. Comprar programas, automatizar formularios o instalar asistentes virtuales no garantiza una transformación administrativa si los procedimientos permanecen fragmentados o si no existen responsabilidades definidas para supervisar los resultados. La tecnología adquiere relevancia pública cuando se integra en procesos institucionales identificables, con objetivos determinados y mecanismos de seguimiento compatibles con las obligaciones administrativas.

Los servicios digitales dirigidos a la ciudadanía constituyen una manifestación visible de esta transformación. Chen et al. (2024) analizan la adopción e implementación de chatbots de inteligencia artificial en organizaciones públicas y muestran cómo estas herramientas pueden incorporarse a la interacción entre instituciones y usuarios. Su utilización puede modificar canales de consulta, orientación y acceso a determinados servicios. Sin embargo, la automatización de la interacción administrativa introduce una cuestión jurídica adicional: la ciudadanía debe poder identificar cuándo está relacionándose con un sistema automatizado y cuáles son sus límites. Esta exigencia adquiere mayor importancia cuando la interacción

tecnológica deja de ser meramente informativa y comienza a influir en procedimientos administrativos.

La expansión de estas herramientas también transforma la gestión de la información pública. Los sistemas de inteligencia artificial requieren datos para identificar patrones, clasificar situaciones o generar resultados, lo que incrementa la importancia jurídica de determinar la procedencia, calidad y finalidad de la información procesada. La Ley Orgánica de Protección de Datos Personales (2021) establece, en su artículo 1, que su objeto es garantizar el ejercicio del derecho a la protección de datos personales, que comprende el acceso y la decisión sobre información y datos de este carácter. Además, su ámbito comprende tratamientos realizados mediante procedimientos automatizados, por lo que la digitalización estatal debe respetar estas garantías.

La transformación digital también introduce vulnerabilidades que deben analizarse antes de ampliar el uso institucional de sistemas inteligentes. Vatamanu y Tofan (2025) examinan desafíos asociados con la integración de inteligencia artificial en la administración pública y advierten que su implementación debe estudiarse junto con sus implicaciones institucionales y jurídicas. La capacidad de procesar grandes cantidades de información puede facilitar determinadas funciones administrativas, pero también puede trasladar errores, criterios deficientes o problemas de diseño a un número elevado de decisiones. Por ello, la escala tecnológica modifica la dimensión del riesgo administrativo: una deficiencia incorporada en un sistema automatizado puede reproducirse sistemáticamente entre numerosos usuarios.

El proceso tampoco puede evaluarse únicamente desde la eficiencia. La Recomendación sobre la Ética de la Inteligencia Artificial de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2021) establece que el desarrollo y uso de sistemas de inteligencia artificial debe respetar los derechos humanos y la dignidad humana, además de considerar principios como transparencia, equidad y supervisión humana. Para la administración pública, este enfoque implica que la modernización tecnológica debe evaluarse según los efectos que produce sobre las personas. Reducir tiempos administrativos puede constituir un resultado positivo, pero no justifica procedimientos automatizados que restrinjan injustificadamente derechos o dificulten comprender una decisión estatal.

En consecuencia, la transformación digital de la administración pública constituye un cambio organizativo y jurídico además de tecnológico. Babšek et al. (2025) muestran que la adopción de inteligencia artificial en la administración pública comprende aplicaciones diversas y un

campo de investigación cada vez más orientado a comprender sus condiciones prácticas de implementación. Esta evolución obliga a mantener una relación coherente entre innovación, capacidad institucional y control jurídico. Las herramientas automatizadas pueden integrarse en distintas fases de la actividad administrativa, pero la responsabilidad pública permanece en las instituciones que las seleccionan, configuran y utilizan. Este punto permite avanzar hacia el análisis específico de la automatización administrativa y sus características dentro de los procesos decisorios estatales.

1.2 Concepto y características de la automatización administrativa

La automatización administrativa puede entenderse como la incorporación de sistemas capaces de ejecutar, apoyar o estructurar tareas que antes dependían de intervención humana directa dentro de una entidad pública. Su alcance comprende desde operaciones rutinarias, como clasificación y registro de información, hasta procesos que influyen en decisiones con efectos jurídicos. Zuiderwijk et al. (2021) señalan que la inteligencia artificial aplicada a la gobernanza pública amplía las posibilidades de procesamiento y apoyo decisorio. En consecuencia, automatizar no equivale únicamente a digitalizar documentos, porque supone trasladar determinadas reglas, criterios o procedimientos administrativos a sistemas capaces de operar con distintos grados de autonomía.

La automatización se diferencia de la digitalización porque esta última puede limitarse a convertir información o trámites a formatos electrónicos sin modificar la lógica del procedimiento. En cambio, un proceso automatizado incorpora instrucciones que permiten al sistema ejecutar acciones, generar resultados o recomendar respuestas a partir de datos definidos. Van Noordt y Misuraca (2022) muestran que la inteligencia artificial gubernamental puede integrarse en distintas funciones públicas y no responde a una única modalidad tecnológica. Por ello, el concepto de automatización administrativa incluye herramientas simples basadas en reglas y sistemas más complejos que utilizan aprendizaje automático para producir inferencias o predicciones.

Una primera característica de la automatización administrativa es su dependencia de reglas, datos y parámetros de funcionamiento. Incluso cuando el sistema emplea modelos capaces de identificar patrones, su operación se encuentra condicionada por decisiones sobre objetivos, variables, fuentes de información y criterios de clasificación. Neumann et al. (2024) evidencian que la adopción de inteligencia artificial en organizaciones públicas depende de condiciones institucionales y organizativas. Esto significa que el resultado automatizado no surge de manera

independiente al entorno administrativo. Las decisiones sobre diseño, adquisición, configuración y uso determinan qué información procesa el sistema y cómo interviene dentro del procedimiento público correspondiente.

Otra característica es la capacidad de automatizar diferentes niveles del proceso decisorio. Un sistema puede limitarse a ordenar expedientes, detectar inconsistencias o priorizar casos, mientras otro puede formular recomendaciones que influyan directamente en la decisión de un servidor público. Alon-Barkat y Busuioc (2023) analizan precisamente la interacción entre funcionarios y asesoramiento algorítmico, mostrando que la automatización también puede operar como apoyo y no como sustitución completa de la decisión humana. Esta distinción resulta jurídicamente relevante porque el grado de intervención del sistema permite identificar dónde se conserva el juicio administrativo y dónde determinadas valoraciones han sido trasladadas a procesos tecnológicos.

La automatización puede ser total o parcial, y esta diferencia posee consecuencias jurídicas relevantes. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas cuando produzca efectos jurídicos o afecte derechos y libertades fundamentales. La norma permite solicitar una explicación motivada, presentar observaciones, conocer criterios de valoración e impugnar la decisión. Por ello, el ordenamiento ecuatoriano no restringe el problema a decisiones automatizadas, sino que también contempla situaciones en las que el procesamiento automatizado participa parcialmente en la valoración realizada.

La capacidad de operar a escala constituye otra característica. Una regla incorporada en un sistema puede aplicarse repetidamente a numerosos expedientes sin que cada caso requiera una ejecución humana equivalente. Esta propiedad puede favorecer uniformidad y rapidez, pero amplifica las consecuencias de errores incorporados en datos, criterios o configuraciones. Vatamanu y Tofan (2025) advierten que la integración de inteligencia artificial en la administración pública presenta vulnerabilidades que deben ser consideradas junto con sus ventajas operativas. Un defecto individual puede corregirse en un caso concreto; en cambio, un defecto automatizado puede reproducirse sistemáticamente mientras permanezca activo dentro del procedimiento institucional correspondiente.

La automatización tampoco elimina necesariamente la intervención humana. Green (2022) cuestiona la idea de que exigir supervisión humana sea una garantía suficiente frente a los problemas derivados de algoritmos gubernamentales. La intervención efectiva requiere que la

persona responsable comprenda el papel del sistema, disponga de información suficiente y tenga capacidad para apartarse de su resultado cuando existan razones justificadas. De lo contrario, la supervisión humana puede convertirse en una validación formal de la recomendación tecnológica. En administración pública, esta característica exige distinguir entre presencia humana nominal y control humano sustantivo, especialmente cuando una decisión puede afectar derechos o intereses legítimos.

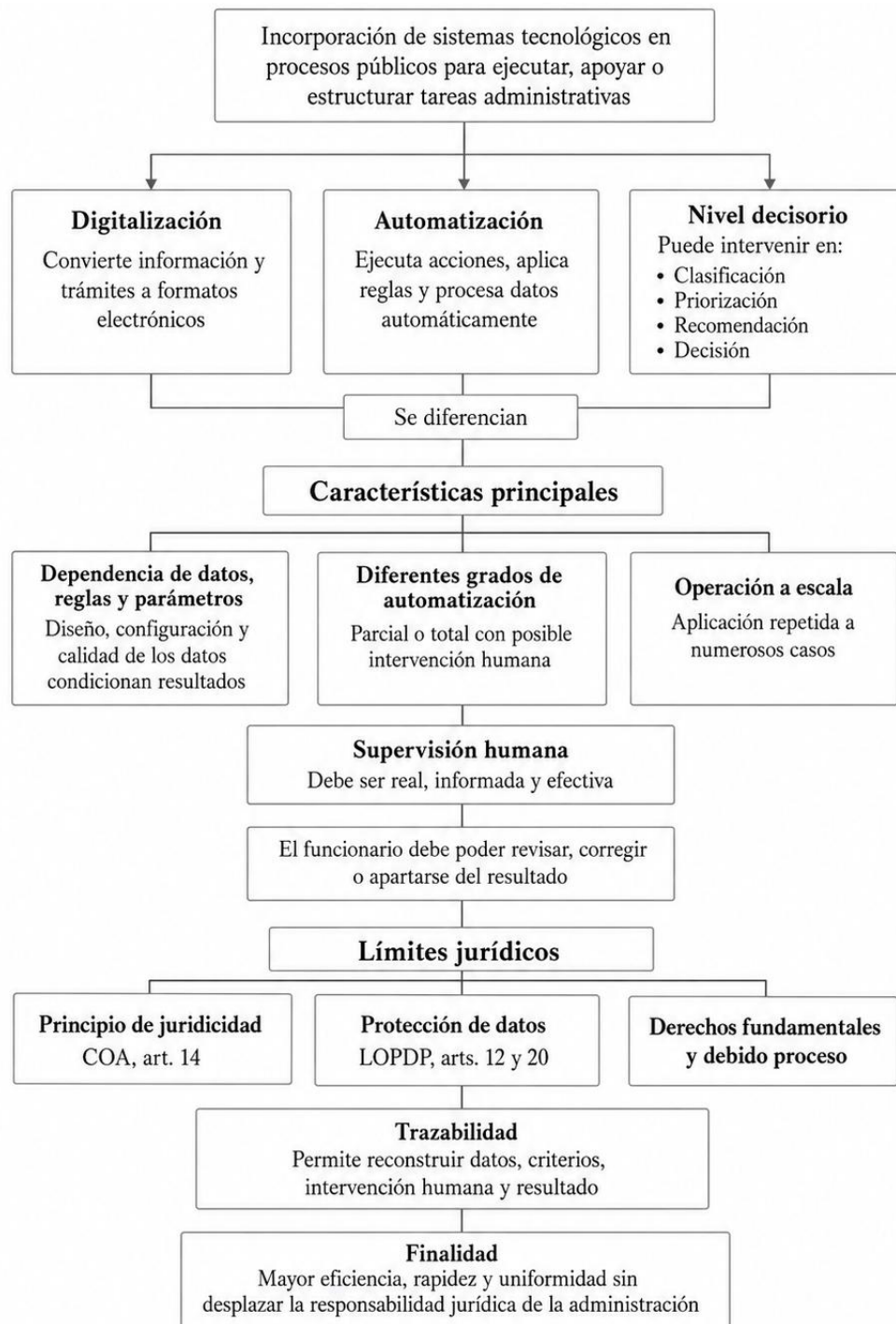
La automatización administrativa se encuentra limitada por el régimen jurídico que regula toda actuación pública. El Código Orgánico Administrativo (2017), en su artículo 14, establece que la actuación administrativa se somete a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. Asimismo, la Constitución de la República del Ecuador (2008), en su artículo 227, dispone que la administración pública se rige, entre otros, por principios de eficacia, eficiencia, calidad, transparencia y evaluación. En consecuencia, la incorporación de automatización no crea un espacio exento de Derecho: el sistema utilizado debe integrarse en competencias, procedimientos y responsabilidades legitimados.

La trazabilidad constituye una característica relevante cuando la automatización interviene en decisiones públicas. Una administración necesita poder reconstruir qué datos fueron utilizados, qué reglas o criterios participaron y qué actuación humana acompañó el resultado generado. Grimmelikhuijsen (2023) vincula la transparencia algorítmica con la percepción de confiabilidad de las decisiones automatizadas, lo que muestra que la comprensibilidad del proceso posee una dimensión institucional además de técnica. La trazabilidad no exige necesariamente revelar cada detalle del funcionamiento interno de un modelo, pero sí conservar información para identificar el recorrido decisorio, revisar errores y explicar comprensiblemente por qué se produjo determinado resultado administrativo.

El uso intensivo de datos añade una característica vinculada con automatización administrativa y protección de derechos. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, el titular debe recibir información sobre finalidades, base legal, tratamiento y existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. Esta obligación muestra que el procesamiento de información no constituye una fase neutral al intervenir en decisiones públicas. La calidad, procedencia y pertinencia de los datos condicionan los resultados producidos. Christodoulou y Limniotis (2024) sitúan la protección de datos entre los desafíos de los sistemas automatizados.

Figura 1

Elementos y características de la automatización administrativa



Nota. El esquema sintetiza las principales características de la automatización administrativa, sus niveles de intervención, mecanismos de supervisión y límites jurídicos aplicables en la gestión pública.

En conjunto, la automatización administrativa se caracteriza por trasladar determinadas operaciones, valoraciones o secuencias procedimentales a sistemas tecnológicos, manteniendo distintos grados de intervención humana. Sus rasgos incluyen dependencia de datos y reglas,

capacidad de repetición a escala, integración en procesos decisorios, posibilidad de funcionamiento parcial o total y necesidad de trazabilidad. Sin embargo, estas propiedades técnicas adquieren significado jurídico únicamente cuando se relacionan con las competencias y obligaciones de la administración. Grimmeliikhuijsen y Meijer (2022) advierten que la legitimidad de la decisión algorítmica enfrenta amenazas institucionales específicas. El análisis debe avanzar, por tanto, hacia las modalidades concretas de aplicación pública.

1.3 Inteligencia artificial y sistemas algorítmicos en la gestión pública

La inteligencia artificial en la gestión pública comprende el uso de sistemas capaces de procesar datos, identificar patrones, generar recomendaciones o intervenir en tareas administrativas con distintos niveles de autonomía. Su presencia puede observarse en clasificación documental, atención ciudadana, detección de riesgos, priorización de expedientes y apoyo a decisiones institucionales. Zuiderwijk et al. (2021) señalan que la inteligencia artificial aplicada a la gobernanza pública puede modificar procesos de prestación de servicios y toma de decisiones. En este sentido, su incorporación no constituye únicamente una innovación tecnológica, porque también altera la forma en que la administración organiza información, distribuye funciones y justifica determinadas actuaciones.

Los sistemas algorítmicos constituyen una categoría más amplia que la inteligencia artificial, ya que incluyen procedimientos programados mediante reglas, modelos estadísticos y mecanismos de aprendizaje automático. Van Noordt y Misuraca (2022) muestran que las aplicaciones gubernamentales de inteligencia artificial presentan grados diversos de complejidad y pueden utilizarse para apoyar funciones administrativas diferentes. Por ello, no toda automatización pública utiliza inteligencia artificial, aunque toda herramienta de inteligencia artificial empleada en la administración depende de algoritmos y datos. Esta diferencia conceptual resulta importante para identificar el nivel de autonomía del sistema, la función que cumple y los riesgos jurídicos asociados con su utilización institucional.

Una característica central de estos sistemas es su capacidad para intervenir en procesos decisorios sin sustituir necesariamente a la persona responsable. Alon-Barkat y Busuioc (2023) analizan la interacción entre funcionarios públicos y recomendaciones algorítmicas y muestran que la decisión humana puede verse influida por el resultado producido por el sistema. Esto obliga a examinar la relación entre asistencia tecnológica y responsabilidad administrativa. Cuando un algoritmo clasifica, prioriza o recomienda, su efecto puede ser significativo aunque formalmente la decisión final corresponda a un servidor público. Por ello, evaluar únicamente

quién firma el acto administrativo puede resultar insuficiente para comprender cómo se construyó realmente la decisión.

En Ecuador, la utilización de inteligencia artificial por entidades públicas debe ajustarse a los principios que regulan la actuación administrativa. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 227, la administración pública debe regirse por principios como eficacia, eficiencia, calidad, transparencia y evaluación. Asimismo, el Código Orgánico Administrativo (2017), en su artículo 14, establece que la actuación administrativa se encuentra sometida a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. En consecuencia, ningún sistema algorítmico puede utilizarse legítimamente al margen de las competencias institucionales y de las garantías previstas en el ordenamiento jurídico.

La utilización de sistemas algorítmicos también exige considerar la protección de datos personales, especialmente cuando el sistema procesa información destinada a generar perfiles, clasificaciones o predicciones. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce derechos frente a decisiones basadas total o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La norma contempla, entre otras garantías, la posibilidad de solicitar explicaciones, presentar observaciones y cuestionar la decisión. Esto demuestra que la gestión pública algorítmica no puede analizarse únicamente desde la eficiencia, porque su diseño y utilización pueden producir consecuencias directas sobre derechos individuales.

Tabla 1

Funciones y riesgos de los sistemas algorítmicos en la gestión pública

Función administrativa	Aplicación algorítmica	Posible utilidad	Riesgo jurídico principal
Atención ciudadana	Chatbots y asistentes virtuales	Respuesta automatizada a consultas	Información incompleta o falta de identificación del sistema
Gestión documental	Clasificación automática de expedientes	Organización y recuperación de información	Errores de clasificación o tratamiento inadecuado de datos
Priorización administrativa	Sistemas de puntuación o riesgo	Ordenamiento de casos según criterios definidos	Sesgos y trato desigual
Apoyo a decisiones	Modelos predictivos o recomendaciones	Análisis de grandes volúmenes de información	Dependencia excesiva de la recomendación automatizada

Control institucional	Detección de anomalías o patrones	Identificación de posibles irregularidades	Falsos positivos y afectación de derechos
Gestión de servicios	Sistemas de asignación automatizada	Distribución de recursos o turnos	Falta de transparencia en los criterios aplicados

Nota. La tabla distingue entre la función administrativa, el uso algorítmico y el principal riesgo jurídico que puede surgir cuando el sistema interviene en procesos públicos.

Los sistemas algorítmicos pueden mejorar determinadas capacidades administrativas cuando permiten procesar información con mayor rapidez o detectar relaciones difíciles de identificar mediante revisión manual. Babšek et al. (2025) muestran que la adopción de inteligencia artificial en la administración pública comprende aplicaciones diversas y se encuentra asociada con procesos de innovación institucional. Sin embargo, la utilidad técnica depende de la calidad de los datos, de la definición de objetivos y de la capacidad de supervisión. Un sistema que opera con información incompleta o criterios poco claros puede producir resultados consistentes desde el punto de vista computacional, pero inadecuados respecto de la finalidad administrativa perseguida.

La transparencia constituye otra exigencia central. Grimmelikhuijsen (2023) evidencia que la transparencia algorítmica influye en la percepción de confiabilidad de las decisiones automatizadas, especialmente cuando las personas intentan comprender por qué el sistema produjo determinado resultado. En el ámbito público, esta exigencia se relaciona con la posibilidad de conocer los criterios relevantes de una actuación administrativa y ejercer control sobre ella. Un sistema técnicamente complejo no puede convertirse en justificación suficiente para negar explicaciones. La administración debe conservar capacidad institucional para identificar los datos utilizados, reconstruir el procedimiento y explicar de manera comprensible el papel que tuvo el sistema en la decisión.

La supervisión humana tampoco debe reducirse a una aprobación automática del resultado generado por el sistema. Green (2022) advierte que las políticas que exigen intervención humana pueden resultar insuficientes cuando la persona encargada no dispone de tiempo, información o capacidad efectiva para cuestionar la recomendación algorítmica. En la gestión pública, una revisión humana significativa exige posibilidad real de analizar el caso, apartarse del resultado y fundamentar una decisión diferente. De lo contrario, la presencia de una persona al final del procedimiento puede funcionar únicamente como formalidad. La responsabilidad administrativa requiere, por tanto, mecanismos de supervisión que permitan controlar efectivamente la intervención tecnológica.

La incorporación de inteligencia artificial y sistemas algorítmicos debe analizarse, finalmente, como una transformación de la estructura decisoria de la administración pública. Vatamanu y Tofan (2025) señalan que su integración genera desafíos y vulnerabilidades que afectan organización, responsabilidad y capacidad institucional. La cuestión central no consiste únicamente en determinar si una herramienta puede automatizar una tarea, sino en establecer bajo qué condiciones jurídicas y administrativas debe hacerlo. La administración continúa siendo responsable de seleccionar, configurar, supervisar y corregir los sistemas que utiliza. Esta responsabilidad constituye el punto de partida para examinar los ámbitos concretos donde las decisiones automatizadas comienzan a intervenir en la actividad pública.

1.4 Ámbitos de aplicación de las decisiones automatizadas en el sector público

Las decisiones automatizadas se aplican en el sector público cuando una institución utiliza sistemas algorítmicos para clasificar información, evaluar situaciones, formular recomendaciones o determinar resultados dentro de procedimientos administrativos. Babšek et al. (2025) identifican aplicaciones de inteligencia artificial vinculadas con servicios públicos, gestión de información, administración interna y apoyo a decisiones. Su utilización puede abarcar desde tareas auxiliares hasta procesos con efectos directos sobre las personas. Por ello, el análisis jurídico debe considerar la función concreta asignada al sistema, los datos utilizados, el grado de intervención humana y las consecuencias que el resultado automatizado puede generar para derechos o intereses individuales.

Un primer ámbito corresponde a la atención y prestación de servicios públicos, donde pueden utilizarse asistentes virtuales, chatbots y mecanismos automatizados para responder consultas, orientar trámites o canalizar solicitudes. Chen et al. (2024) muestran que estas herramientas han sido incorporadas por organizaciones públicas como medios de interacción con la ciudadanía. Aunque muchas de sus funciones son informativas, pueden influir en el acceso efectivo a prestaciones cuando orientan sobre requisitos, plazos o procedimientos. La administración debe asegurar que la automatización no dificulte el acceso de personas con necesidades particulares y que siempre existan mecanismos adecuados para corregir información incorrecta o insuficiente proporcionada automáticamente.

Otro ámbito de aplicación se encuentra en la gestión y clasificación de expedientes administrativos. Los algoritmos pueden organizar documentos, identificar información relevante, detectar inconsistencias y asignar prioridades según criterios previamente definidos. Yigitcanlar et al. (2024) muestran que los gobiernos locales emplean inteligencia artificial en

una diversidad de funciones administrativas y servicios. Estas herramientas pueden reducir tareas repetitivas y facilitar el procesamiento de grandes cantidades de información, pero su funcionamiento depende de datos y reglas que deben ser revisables. Si un sistema clasifica erróneamente una solicitud o asigna una prioridad inadecuada, el error tecnológico puede afectar posteriormente el desarrollo del procedimiento administrativo.

La asignación de prestaciones, ayudas o recursos públicos constituye un ámbito especialmente sensible. Los sistemas automatizados pueden emplearse para verificar requisitos, identificar posibles beneficiarios, establecer puntuaciones o detectar incompatibilidades entre datos proporcionados y registros administrativos. En estos casos, la automatización puede afectar directamente la posibilidad de acceder a una prestación estatal. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, reconoce la igualdad de las personas y prohíbe la discriminación por diversas condiciones personales o sociales. En consecuencia, cualquier sistema utilizado para distribuir recursos públicos debe evitar criterios que produzcan exclusiones discriminatorias directas o indirectas.

Los sistemas automatizados también pueden intervenir en actividades de inspección, control y detección de irregularidades. Mediante análisis de patrones, una institución puede identificar operaciones atípicas, inconsistencias documentales o casos que requieren una revisión prioritaria. Vatamanu y Tofan (2025) advierten que la incorporación de inteligencia artificial en la administración pública genera vulnerabilidades relacionadas con la calidad de los datos, la responsabilidad y el funcionamiento institucional. En este ámbito, un resultado algorítmico debería entenderse como un elemento para orientar una actuación posterior y no necesariamente como prueba concluyente de incumplimiento. La existencia de falsos positivos exige mecanismos de contraste antes de imponer consecuencias administrativas.

La gestión tributaria constituye otro espacio donde pueden emplearse herramientas automatizadas para analizar declaraciones, identificar riesgos, cruzar información y seleccionar casos sujetos a revisión. Su aplicación permite procesar grandes volúmenes de datos que serían difíciles de examinar individualmente mediante métodos manuales. Sin embargo, cuando una clasificación algorítmica aumenta la probabilidad de fiscalización o influye en una determinación administrativa, debe existir una base jurídica clara para su utilización. El Código Orgánico Administrativo (2017), en su artículo 14, dispone que toda actuación administrativa está sometida a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable.

En materia de seguridad y gestión urbana, los sistemas algorítmicos pueden utilizarse para analizar movilidad, identificar patrones de riesgo, gestionar infraestructura o apoyar decisiones relacionadas con ciudades inteligentes. Ameen et al. (2026) examinan precisamente los problemas de legalidad, evidencia y mecanismos de reparación vinculados con sistemas administrativos algorítmicos utilizados en entornos urbanos inteligentes. La utilización de estos instrumentos puede producir efectos sobre movilidad, vigilancia, acceso a espacios o intervención administrativa. Por ello, el hecho de que una tecnología opere sobre datos urbanos no elimina la necesidad de controlar proporcionalidad, competencia institucional, calidad de la información y posibilidades de impugnación cuando una persona resulte afectada.

La gestión de datos personales constituye un componente transversal en numerosos ámbitos de automatización pública. Los sistemas utilizados para prestaciones, fiscalización, seguridad, salud o planificación pueden requerir información vinculada con personas identificadas o identificables. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece principios aplicables al tratamiento, entre ellos juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad, confidencialidad y calidad de los datos. Estos principios limitan la cantidad y el tipo de información que puede utilizar una institución, incluso cuando el procesamiento automatizado resulte técnicamente posible o administrativamente conveniente para alcanzar determinados objetivos públicos.

El ámbito sanitario también puede incorporar sistemas destinados a apoyar clasificación de pacientes, asignación de recursos, análisis de riesgos o procesamiento de información clínica. Murdoch (2021) advierte que la utilización de inteligencia artificial plantea problemas específicos para la privacidad cuando implica grandes volúmenes de información personal sensible. En Ecuador, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 25, incluye los datos relativos a la salud dentro de las categorías especiales de datos personales. Esto exige controles reforzados cuando sistemas automatizados intervienen en procedimientos públicos sanitarios, debido a las consecuencias que una utilización inadecuada puede generar sobre intimidad, confidencialidad y ejercicio de derechos.

Las decisiones automatizadas también pueden emplearse para apoyar a servidores públicos encargados de resolver expedientes. En estos casos, el algoritmo no determina formalmente la decisión, pero puede emitir puntuaciones, clasificaciones, alertas o recomendaciones que influyen en el juicio humano. Alon-Barkat y Busuioc (2023) analizaron experimentalmente la relación entre funcionarios y asesoramiento algorítmico, mostrando la importancia de estudiar cómo las personas procesan estas recomendaciones. La existencia de un funcionario al final

del procedimiento no garantiza por sí misma una valoración independiente. La supervisión requiere capacidad para comprender el resultado, identificar sus limitaciones y apartarse razonadamente de la recomendación cuando las circunstancias del caso lo exijan.

La diversidad de ámbitos demuestra que las decisiones automatizadas pueden intervenir tanto en tareas internas como en actuaciones capaces de afectar directamente derechos. Por ello, su evaluación debe atender al nivel de riesgo y al impacto jurídico de cada aplicación, evitando tratar todas las herramientas como equivalentes. La Constitución de la República del Ecuador (2008), en su artículo 227, exige que la administración pública actúe conforme a principios de eficacia, eficiencia, calidad, transparencia y evaluación. La automatización puede contribuir a estos objetivos, pero permanece sometida a las obligaciones institucionales existentes. Su legitimidad dependerá de que tecnología, procedimiento y garantías jurídicas permanezcan articulados dentro de la actuación pública.

1.5 Eficiencia administrativa y límites de la automatización

La eficiencia administrativa constituye una finalidad legítima de la transformación digital, pero no puede analizarse al margen de las obligaciones jurídicas que regulan la actuación estatal. La Constitución de la República del Ecuador (2008), en su artículo 227, establece que la administración pública debe regirse, entre otros, por los principios de eficacia, eficiencia, calidad, transparencia y evaluación. La automatización puede contribuir a reducir tiempos, procesar grandes volúmenes de información y estandarizar determinadas tareas. Sin embargo, estos beneficios operativos no autorizan a sustituir las garantías jurídicas por criterios exclusivamente técnicos, porque la eficiencia constituye uno de varios principios que deben observarse simultáneamente.

La incorporación de sistemas automatizados puede mejorar la capacidad institucional para clasificar expedientes, detectar inconsistencias y orientar recursos hacia actividades prioritarias. Babšek et al. (2025) identifican diversas aplicaciones de inteligencia artificial dentro de la administración pública, mientras que Vatamanu y Tofan (2025) advierten que su integración también introduce vulnerabilidades organizativas y jurídicas. En consecuencia, la valoración de eficiencia no debería limitarse al número de trámites procesados o al tiempo ahorrado. También debe considerar la calidad del resultado, la posibilidad de corregir errores, la protección de derechos y los costos institucionales derivados de decisiones automatizadas deficientes o difíciles de revisar.

El primer límite jurídico de la automatización administrativa deriva del principio de juridicidad. De acuerdo con el Código Orgánico Administrativo (2017), en su artículo 14, la actuación administrativa se encuentra sometida a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. Esto significa que una institución no puede utilizar un sistema automatizado para introducir requisitos, criterios de exclusión o consecuencias que carezcan de respaldo normativo. La programación tecnológica debe responder a competencias previamente atribuidas a la administración. Por tanto, la automatización puede modificar la forma de ejecutar un procedimiento, pero no puede ampliar discrecionalmente las potestades legales de la autoridad pública.

Un segundo límite aparece cuando la automatización afecta derechos individuales. La Constitución de la República del Ecuador (2008), en su artículo 76, reconoce garantías del debido proceso en toda actuación en la que se determinen derechos y obligaciones. Esta exigencia mantiene su vigencia aunque una fase del procedimiento sea realizada mediante algoritmos. Green (2022) cuestiona que la simple presencia de supervisión humana constituya una garantía suficiente si la persona responsable carece de capacidad real para revisar el resultado tecnológico. En consecuencia, eficiencia y automatización deben coexistir con posibilidades efectivas de contradicción, revisión y decisión humana cuando la actuación pueda producir consecuencias jurídicas desfavorables para una persona.

La protección de datos establece otro límite sustantivo. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que el tratamiento observe principios como juridicidad, transparencia, finalidad, minimización, proporcionalidad y calidad. Además, su artículo 20 reconoce garantías frente a decisiones basadas total o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La eficiencia obtenida mediante acumulación masiva de información no justifica utilizar datos innecesarios o inadecuados. Christodoulou y Limniotis (2024) muestran que los sistemas automatizados basados en aprendizaje automático plantean desafíos específicos para la aplicación efectiva de las reglas de protección de datos.

Tabla 2

Relación entre eficiencia administrativa y límites jurídicos de la automatización

Dimensión de eficiencia	Posible aporte de la automatización	Límite jurídico	Fundamento principal
Rapidez	Procesamiento acelerado de solicitudes	No reducir garantías procedimentales	Constitución, art. 76

Productividad	Automatización de tareas repetitivas	Actuación dentro de competencias legales	Código Orgánico Administrativo, art. 14
Uso de datos	Análisis de grandes volúmenes de información	Finalidad, minimización, proporcionalidad y calidad	Ley Orgánica de Protección de Datos Personales, art. 10
Decisión	Clasificación, puntuación o recomendación automatizada	Derechos frente a valoraciones automatizadas	Ley Orgánica de Protección de Datos Personales, art. 20
Uniformidad	Aplicación constante de criterios	Prevención de resultados discriminatorios	Constitución, art. 11, núm. 2
Control	Detección automatizada de riesgos o anomalías	Explicabilidad, revisión y responsabilidad	UNESCO, 2021, párrs. 37–43

Nota. La eficiencia administrativa debe evaluarse junto con los límites derivados de juridicidad, debido proceso, igualdad, protección de datos, transparencia y responsabilidad institucional.

La automatización tampoco puede justificarse cuando sus efectos comprometen el principio de igualdad. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, reconoce la igualdad de todas las personas y prohíbe la discriminación. Este mandato resulta relevante porque un sistema aparentemente uniforme puede generar consecuencias diferenciadas si utiliza datos históricos o variables que reproducen desigualdades. Lendvai y Gosztonyi (2025) analizan el sesgo algorítmico como un problema jurídico asociado con sistemas de inteligencia artificial. La administración debe valorar, por tanto, si la búsqueda de eficiencia produce distribuciones injustificadas de beneficios, cargas, controles o probabilidades de acceso a servicios públicos.

La proporcionalidad permite delimitar cuándo resulta razonable automatizar una función administrativa. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021), en sus párrafos 25 y 26, establece que la elección de utilizar inteligencia artificial debe ser apropiada y proporcional al objetivo legítimo perseguido y no debe vulnerar derechos humanos. Además, sus párrafos 35 y 36 sostienen que la responsabilidad última no puede trasladarse al sistema tecnológico. En consecuencia, no todas las tareas deben automatizarse simplemente porque exista capacidad técnica para hacerlo. Las instituciones deben justificar que la tecnología seleccionada resulta adecuada al contexto, al riesgo y a las consecuencias esperadas.

La experiencia regulatoria comparada refuerza esta necesidad de establecer controles diferenciados según el riesgo. El Reglamento (UE) 2024/1689 contempla obligaciones

específicas para sistemas de inteligencia artificial de alto riesgo: su artículo 9 exige un sistema de gestión de riesgos y el artículo 14 establece medidas de supervisión humana. Estas disposiciones no constituyen derecho ecuatoriano, pero ofrecen un parámetro comparativo útil para comprender que la eficiencia tecnológica debe acompañarse de mecanismos institucionales de prevención y control. La automatización de una actividad rutinaria no presenta el mismo nivel de riesgo que un sistema utilizado para determinar acceso a prestaciones, fiscalización o ejercicio de derechos.

En definitiva, la eficiencia administrativa puede justificar la adopción de herramientas automatizadas únicamente cuando su utilización permanece subordinada al ordenamiento jurídico y a la protección efectiva de derechos. Sanchez-Graells (2024) sostiene que la digitalización del sector público obliga a reconsiderar cómo se preservan las garantías de buena administración frente a efectos masivos producidos por tecnologías digitales. La rapidez, uniformidad y reducción de costos deben evaluarse junto con juridicidad, proporcionalidad, transparencia, revisión humana y responsabilidad. La automatización pierde legitimidad cuando los beneficios operativos dependen de reducir garantías o dificultar la impugnación. El criterio decisivo debe ser una administración eficiente que continúe siendo jurídicamente controlable y responsable.

1.6 Riesgos de la delegación de decisiones públicas a sistemas automatizados

La delegación de decisiones públicas a sistemas automatizados introduce riesgos que trascienden los problemas estrictamente técnicos, porque las actuaciones estatales pueden determinar derechos, prestaciones, sanciones, prioridades o cargas para las personas. Cuando un algoritmo participa en estas decisiones, parte del razonamiento administrativo puede quedar incorporado en reglas, modelos o parámetros difíciles de observar directamente. Alon-Barkat y Busuioc (2023) muestran que las recomendaciones algorítmicas pueden influir en el comportamiento de los funcionarios públicos, incluso cuando estos conservan formalmente la decisión final. Por ello, la automatización requiere examinar quién decide realmente, cómo se forma el resultado y quién responde por sus consecuencias.

Uno de los principales riesgos consiste en trasladar indebidamente la responsabilidad desde la autoridad pública hacia el sistema tecnológico. La existencia de un algoritmo no modifica la obligación institucional de responder por las decisiones adoptadas dentro del ejercicio de competencias públicas. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021), en sus párrafos 35 y 36, establece que debe ser posible atribuir

responsabilidad ética y jurídica durante todo el ciclo de vida de los sistemas de inteligencia artificial y que estos no deben recibir personalidad jurídica propia. En consecuencia, una administración no puede justificar un resultado perjudicial argumentando simplemente que fue producido por un algoritmo.

Otro riesgo se relaciona con la pérdida de control humano efectivo. Green (2022) cuestiona las políticas que consideran suficiente incorporar una persona al final del procedimiento, porque la supervisión puede convertirse en una formalidad cuando el funcionario carece de información, tiempo o autoridad para revisar el resultado. La UNESCO (2021), en los párrafos 37 a 40 de su Recomendación, relaciona la supervisión humana con transparencia, información y posibilidad de revisión. Esto implica que la intervención humana debe ser sustantiva: el servidor público necesita comprender las limitaciones del sistema, valorar las circunstancias particulares y disponer de capacidad real para apartarse de una recomendación automatizada.

La automatización también puede producir una aceptación acrítica de resultados algorítmicos. Alon-Barkat y Busuioc (2023) estudian el denominado sesgo de automatización y muestran que la interacción entre funcionarios y recomendaciones algorítmicas puede modificar el proceso decisorio. El problema aparece cuando la autoridad atribuye al sistema un grado de precisión o neutralidad que no ha sido suficientemente demostrado. En tales condiciones, una recomendación puede terminar funcionando como decisión de hecho, aunque jurídicamente permanezca atribuida a una persona. Este riesgo exige establecer procedimientos que obliguen a contrastar resultados, documentar discrepancias y evitar que la confianza tecnológica sustituya el análisis individual de cada expediente administrativo.

La reproducción de discriminaciones constituye otro riesgo relevante. Los sistemas automatizados pueden utilizar información histórica que refleje desigualdades previas o variables aparentemente neutrales que produzcan efectos diferenciados sobre determinados grupos. Lendvai y Gosztanyi (2025) analizan el sesgo algorítmico como un problema jurídico que exige respuestas regulatorias específicas. En Ecuador, la Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, reconoce la igualdad de todas las personas, prohíbe la discriminación y dispone que el Estado adopte medidas de acción afirmativa cuando corresponda. Por tanto, la automatización no puede utilizarse legítimamente cuando reproduce distinciones incompatibles con este mandato constitucional.

La delegación algorítmica puede afectar además el derecho al debido proceso cuando la persona desconoce cómo se produjo una decisión que modifica su situación jurídica. De

acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 76, en todo proceso en el que se determinen derechos y obligaciones debe asegurarse el debido proceso. Una decisión automatizada que no permita conocer criterios relevantes, controvertir información incorrecta o presentar argumentos puede debilitar estas garantías. La complejidad técnica no elimina las obligaciones procedimentales de la administración. Si el sistema interviene materialmente en la determinación del resultado, su utilización debe permitir que la persona afectada ejerza defensa efectiva frente a la actuación estatal.

La opacidad constituye un riesgo adicional porque puede impedir reconstruir el razonamiento que condujo al resultado administrativo. Cheong (2024) relaciona transparencia y rendición de cuentas con la protección de las personas frente a sistemas de inteligencia artificial, mientras que Grimmelikhuijsen (2023) muestra que la transparencia algorítmica influye en la percepción de confiabilidad de las decisiones automatizadas. En el sector público, este problema adquiere una dimensión jurídica: una persona debe poder comprender las razones relevantes de una actuación que afecta sus derechos. Cuando ni funcionarios ni ciudadanos pueden identificar datos, criterios o factores determinantes, la posibilidad de controlar la legalidad de la decisión disminuye considerablemente.

El tratamiento masivo de información personal representa igualmente un riesgo cuando la automatización requiere integrar registros procedentes de diversas instituciones. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige principios como juridicidad, transparencia, finalidad, minimización, proporcionalidad y calidad durante el tratamiento de datos. Además, su artículo 20 reconoce derechos frente a decisiones basadas total o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La delegación tecnológica, por tanto, no autoriza a recopilar información ilimitada ni utilizar datos para finalidades diferentes de aquellas que justificaron jurídicamente su tratamiento.

Un riesgo especialmente importante aparece cuando los errores se reproducen a gran escala. Mientras una equivocación humana puede limitarse a un expediente concreto, un criterio incorrecto incorporado en un sistema automatizado puede aplicarse repetidamente a cientos o miles de personas. Sanchez-Graells (2024) analiza precisamente los efectos masivos que puede generar la digitalización del sector público y la necesidad de preservar las garantías de buena administración. Esta capacidad de reproducción obliga a desarrollar mecanismos de auditoría, monitoreo y corrección temprana. No basta con revisar decisiones individualmente después de

producirse el daño, porque determinados errores estructurales requieren identificar y modificar las reglas, datos o configuraciones que los generan sistemáticamente.

Figura 2

Riesgos de la delegación de decisiones públicas a sistemas automatizados



Nota. El esquema sintetiza los principales riesgos asociados con la delegación de decisiones públicas a sistemas automatizados y las respuestas institucionales necesarias para garantizar supervisión, transparencia, protección de datos y respeto de los derechos humanos.

La delegación también puede debilitar el principio de juridicidad cuando criterios tecnológicos comienzan a sustituir condiciones establecidas normativamente. De acuerdo con el Código Orgánico Administrativo (2017), en su artículo 14, la actuación administrativa debe someterse a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. Por ello, una puntuación de riesgo, clasificación algorítmica o indicador predictivo no puede crear por sí mismo una nueva causal de exclusión, sanción o restricción. El sistema debe operar dentro de las competencias y condiciones establecidas jurídicamente. La programación administrativa constituye una forma de ejecución institucional y, por consiguiente, también está sometida al principio de juridicidad.

La delegación de decisiones públicas a sistemas automatizados exige, finalmente, conservar mecanismos efectivos de control, revisión y responsabilidad. La eficiencia tecnológica pierde legitimidad cuando dificulta identificar responsables, cuestionar resultados o reparar

afectaciones. La UNESCO (2021), en sus párrafos 35 a 40, vincula responsabilidad, supervisión humana, transparencia y posibilidad de revisión como componentes de una gobernanza responsable de la inteligencia artificial. Teo (2025) advierte, desde una perspectiva de derechos humanos, que los impactos de la inteligencia artificial pueden acumularse de forma progresiva y afectar distintas garantías. La automatización pública debe permanecer subordinada a instituciones capaces de explicar, revisar, corregir y asumir jurídicamente sus decisiones.

1.7 Derechos humanos como límite y criterio de la transformación digital pública

La transformación digital de la administración pública debe desarrollarse dentro de un marco jurídico orientado por los derechos humanos. La incorporación de inteligencia artificial, algoritmos y sistemas automatizados no modifica la obligación estatal de respetar y garantizar los derechos reconocidos constitucionalmente. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 9, establece que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución. En consecuencia, la modernización tecnológica pierde legitimidad cuando una mejora operativa produce restricciones injustificadas, discriminación, pérdida de privacidad o dificultades para ejercer defensa frente a decisiones administrativas automatizadas.

El principio de igualdad constituye uno de los primeros límites materiales de la automatización pública. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, reconoce que todas las personas son iguales y prohíbe la discriminación basada en condiciones personales, sociales o de otra naturaleza. Este mandato resulta particularmente relevante cuando los algoritmos clasifican ciudadanos, establecen puntuaciones o priorizan solicitudes. Lendvai y Gosztonyi (2025) analizan el sesgo algorítmico como un problema jurídico vinculado con la capacidad de los sistemas de inteligencia artificial para reproducir desigualdades. La neutralidad técnica, por tanto, no puede presumirse únicamente por utilizar procedimientos computacionales.

La protección de la privacidad y de los datos personales constituye otro criterio obligatorio. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce el derecho a la protección de datos personales, incluido el acceso y decisión sobre información de este carácter. Este derecho se desarrolla en la Ley Orgánica de Protección de Datos Personales (2021), cuyo artículo 10 establece principios de juridicidad, lealtad, transparencia, finalidad, minimización, proporcionalidad, confidencialidad y calidad. En consecuencia, una

institución pública no debería incorporar datos a sistemas automatizados simplemente porque tecnológicamente pueda procesarlos, sino únicamente cuando exista justificación jurídica y necesidad respecto de la finalidad administrativa perseguida.

Los derechos humanos también condicionan la forma en que se adoptan decisiones capaces de producir efectos jurídicos. La Constitución de la República del Ecuador (2008), en su artículo 76, dispone que en todo proceso en el que se determinen derechos y obligaciones debe garantizarse el debido proceso. En materia específicamente automatizada, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce derechos frente a decisiones basadas única o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. Esto incluye posibilidades de explicación, observación e impugnación, esenciales para impedir que la tecnología convierta una decisión pública en un resultado incuestionable.

La perspectiva internacional refuerza este enfoque centrado en derechos. La Recomendación sobre la Ética de la Inteligencia Artificial de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2021) establece que el respeto, protección y promoción de los derechos humanos y de la dignidad deben acompañar el ciclo de vida de los sistemas de inteligencia artificial. Asimismo, sus párrafos 35 y 36 señalan la necesidad de mantener mecanismos de responsabilidad, mientras que el párrafo 43 incorpora la importancia de supervisión, auditabilidad y reparación frente a daños derivados del uso de inteligencia artificial. Estos estándares constituyen criterios relevantes para orientar una transformación digital pública jurídicamente responsable.

Tabla 3

Derechos humanos como límites de la transformación digital pública

Derecho o garantía	Riesgo asociado con la automatización	Criterio jurídico aplicable	Fundamento principal
Igualdad y no discriminación	Sesgos en clasificación, priorización o acceso a servicios	Evaluar impactos diferenciados y evitar criterios discriminatorios	Constitución, art. 11, núm. 2
Protección de datos	Recolección excesiva o reutilización injustificada	Finalidad, minimización, proporcionalidad y calidad	Constitución, art. 66, núm. 19; LOPDP, art. 10
Debido proceso	Imposibilidad de conocer o cuestionar una decisión	Garantizar defensa, contradicción y revisión	Constitución, art. 76

Derecho o garantía	Riesgo asociado con la automatización	Criterio jurídico aplicable	Fundamento principal
Protección frente a decisiones automatizadas	Efectos jurídicos derivados de perfiles o valoraciones algorítmicas	Explicación, observación e impugnación	LOPDP, art. 20
Tutela efectiva	Dificultades para reclamar frente a una afectación	Acceso a mecanismos efectivos de protección	Constitución, art. 75
Responsabilidad institucional	Traslado de responsabilidad al algoritmo o proveedor	Mantener responsabilidad humana e institucional	UNESCO, 2021, párrs. 35–36
Reparación	Daños producidos por decisiones automatizadas	Auditoría, revisión y mecanismos de reparación	UNESCO, 2021, párr. 43

Nota. Los derechos humanos operan como condiciones jurídicas que deben observarse durante el diseño, implementación, utilización y revisión de sistemas automatizados en la administración pública.

La tutela efectiva adquiere especial relevancia cuando una decisión tecnológica produce una afectación individual. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho al acceso gratuito a la justicia y a una tutela efectiva, imparcial y expedita de los derechos e intereses. Este mandato exige que una persona pueda cuestionar una decisión pública incluso cuando su origen material se encuentre en un sistema automatizado. Bayamlioğlu (2022) sostiene que el derecho a controvertir decisiones automatizadas posee una función distinta de la mera explicación, porque permite discutir el resultado y sus fundamentos. La tecnología no puede convertirse en una barrera para acceder a mecanismos efectivos de reclamación.

La seguridad jurídica constituye otro parámetro necesario. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 82, este derecho se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por autoridades competentes. Una decisión automatizada resulta problemática cuando incorpora criterios que la persona no podía conocer, reglas diferentes de las previstas normativamente o modelos cuya aplicación modifica materialmente los requisitos del procedimiento. Sanchez-Graells (2024) advierte que la digitalización del sector público puede producir efectos masivos que requieren preservar las garantías tradicionales de buena administración frente a nuevas formas tecnológicas de actuación.

Desde una perspectiva comparada, el Reglamento (UE) 2024/1689 confirma la tendencia hacia una regulación basada en riesgos y derechos fundamentales. Su artículo 9 establece

obligaciones de gestión de riesgos para sistemas considerados de alto riesgo, mientras que su artículo 14 exige mecanismos de supervisión humana adecuados durante su utilización. Aunque estas disposiciones no constituyen legislación ecuatoriana, ofrecen un parámetro útil para analizar sistemas públicos capaces de afectar significativamente derechos. El enfoque demuestra que el control jurídico debe intensificarse cuando aumenta la capacidad del sistema para influir en decisiones relevantes sobre personas, especialmente cuando interviene en acceso a servicios, evaluación, clasificación o ejercicio de potestades públicas.

Los derechos humanos deben funcionar, finalmente, como criterio de diseño y evaluación de la transformación digital pública, y no únicamente como mecanismo correctivo posterior. Teo (2025) advierte que determinados impactos de la inteligencia artificial sobre los derechos pueden acumularse progresivamente, mientras que Cheong (2024) vincula transparencia y responsabilidad con la protección frente a decisiones algorítmicas. Esto exige evaluar los sistemas antes de implementarlos, supervisarlos durante su funcionamiento y corregirlos cuando aparezcan efectos incompatibles con derechos. La transformación digital será jurídicamente admisible cuando la tecnología fortalezca la capacidad administrativa sin reducir igualdad, privacidad, debido proceso, tutela efectiva, seguridad jurídica ni responsabilidad institucional.

Capítulo 2

Igualdad y no discriminación algorítmica

Jessica Jessennia Moreno Acosta



2.1 Principio de igualdad y prohibición de discriminación en la actuación pública

El principio de igualdad constituye un límite jurídico obligatorio para toda actuación de la administración pública, incluidas aquellas desarrolladas mediante sistemas automatizados. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, establece que todas las personas son iguales, gozan de los mismos derechos, deberes y oportunidades, y prohíbe la discriminación por diversas condiciones personales y sociales. Este mandato obliga a las instituciones públicas a examinar tanto las diferencias expresas de trato como los efectos que sus procedimientos pueden generar. En consecuencia, la utilización de algoritmos no modifica la obligación constitucional de asegurar un ejercicio igualitario de los derechos.

La igualdad constitucional comprende una dimensión que supera la aplicación idéntica de una regla a todas las personas. El artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) dispone además que el Estado debe adoptar medidas de acción afirmativa destinadas a promover la igualdad real en favor de quienes se encuentren en situación de desigualdad. De forma complementaria, el artículo 66, numeral 4, reconoce el derecho a la igualdad formal, igualdad material y no discriminación. Estos mandatos resultan relevantes para la automatización pública porque una regla algorítmica uniforme puede producir efectos desiguales cuando opera sobre condiciones sociales previamente diferenciadas.

La prohibición de discriminación también obliga a examinar cómo se construyen los criterios utilizados para clasificar, priorizar o excluir personas dentro de procedimientos administrativos. Wang et al. (2024) identifican diferentes manifestaciones de discriminación algorítmica, entre ellas aquella relacionada con selección de características, variables sustitutivas y efectos diferenciados generados por sistemas automatizados. Estas formas de discriminación muestran que el problema no siempre aparece mediante una regla explícitamente excluyente. Un algoritmo puede utilizar variables aparentemente neutrales y, aun así, producir una distribución sistemáticamente desfavorable para determinados grupos. Por ello, la administración debe evaluar tanto la formulación del criterio como sus consecuencias prácticas.

La actuación pública tampoco puede justificar diferencias de trato únicamente porque hayan sido generadas mediante procedimientos tecnológicos. El artículo 24 de la Convención Americana sobre Derechos Humanos (1969) reconoce que todas las personas son iguales ante la ley y tienen derecho, sin discriminación, a igual protección jurídica. A su vez, su artículo 1.1 obliga a los Estados partes a respetar y garantizar los derechos reconocidos en la Convención

sin discriminación. Estos estándares son aplicables a las actuaciones estatales independientemente del instrumento empleado para ejecutarlas. Por ello, una clasificación producida por inteligencia artificial continúa siendo jurídicamente atribuible a la institución que decide utilizarla.

El Pacto Internacional de Derechos Civiles y Políticos (1966) refuerza esta obligación desde el sistema universal de derechos humanos. Su artículo 26 reconoce que todas las personas son iguales ante la ley y tienen derecho, sin discriminación, a igual protección legal. Esta disposición posee particular importancia frente a sistemas automatizados utilizados por instituciones estatales, debido a que la igualdad debe examinarse en función de los resultados concretos que produce la actuación pública. Si una herramienta asigna diferentes probabilidades de acceso, control, revisión o exclusión sobre la base de características protegidas o variables estrechamente relacionadas con ellas, su utilización requiere una justificación jurídicamente suficiente.

La Declaración Universal de Derechos Humanos (1948) establece igualmente un fundamento general para la prohibición de discriminación. Su artículo 2 reconoce los derechos y libertades sin distinción basada en condiciones como raza, sexo, idioma, religión, opinión, origen o situación personal, mientras que su artículo 7 proclama la igualdad ante la ley y la protección contra toda discriminación. Aunque la Declaración posee una naturaleza jurídica distinta de los tratados ratificados por los Estados, constituye un referente central del sistema internacional de derechos humanos. Estas disposiciones permiten comprender que la innovación administrativa debe mantenerse subordinada a condiciones básicas de igualdad y protección jurídica de las personas.

Los sistemas de inteligencia artificial pueden generar dificultades adicionales para aplicar estos principios porque las diferencias de trato no siempre resultan fácilmente observables. Lütz (2022) analiza cómo los sesgos algorítmicos pueden producir impactos directos e indirectos sobre la igualdad de género y advierte que los marcos tradicionales de no discriminación deben enfrentarse a formas de decisión mediadas por algoritmos. En la actuación pública, este problema exige observar qué variables intervienen en una decisión, cómo fueron seleccionadas y qué efectos producen sobre distintos grupos. La ausencia de una referencia explícita al sexo, origen u otra característica protegida no demuestra, por sí sola, ausencia de discriminación.

La igualdad también requiere controlar la calidad y representatividad de los datos utilizados por la administración. Un sistema entrenado con información histórica puede aprender

relaciones construidas bajo condiciones sociales desiguales y reproducirlas posteriormente como si fueran predicciones neutrales. Wang et al. (2024) explican que la discriminación algorítmica puede aparecer mediante múltiples mecanismos, incluidos criterios de selección de variables, impactos dispares y el empleo de información que funciona como sustituto de características protegidas. En consecuencia, evaluar un sistema únicamente a partir de su precisión promedio resulta insuficiente. La administración debe comprobar cómo distribuye errores, beneficios, cargas y oportunidades entre diferentes grupos de población.

La prohibición de discriminación exige además que las instituciones públicas mantengan capacidad efectiva para revisar los sistemas que utilizan. La Constitución de la República del Ecuador (2008), en su artículo 226, establece que las instituciones del Estado y quienes ejercen potestad pública solo pueden ejercer las competencias y facultades atribuidas por la Constitución y la ley. Por su parte, el artículo 227 dispone que la administración pública debe regirse, entre otros, por los principios de calidad, transparencia y evaluación. Estas reglas impiden considerar al algoritmo como un agente independiente de la institución y obligan a mantener mecanismos de evaluación sobre los efectos de su utilización administrativa.

La igualdad algorítmica tampoco puede reducirse a una propiedad matemática del sistema. Una herramienta puede satisfacer determinado indicador estadístico y, sin embargo, generar un resultado jurídicamente problemático si la diferencia de trato carece de una finalidad legítima o afecta de manera desproporcionada a determinadas personas. Lütz (2022) muestra que los conceptos jurídicos de igualdad y discriminación no pueden sustituirse automáticamente por criterios técnicos de equidad algorítmica. Teo (2025), desde una perspectiva de derechos humanos, advierte además que ciertos efectos de la inteligencia artificial pueden acumularse y dificultar la identificación y exigencia de responsabilidad. El análisis debe integrar, por tanto, dimensiones técnicas, jurídicas e institucionales.

En la administración pública, el principio de igualdad funciona simultáneamente como límite, obligación de actuación y criterio para evaluar sistemas automatizados. No basta con que una herramienta aplique la misma regla formal a todos los expedientes; es necesario examinar si esa regla produce exclusiones, cargas o beneficios diferenciados carentes de justificación. La Constitución de la República del Ecuador (2008), en sus artículos 11, numeral 2, y 66, numeral 4, junto con el artículo 24 de la Convención Americana sobre Derechos Humanos (1969) y el artículo 26 del Pacto Internacional de Derechos Civiles y Políticos (1966), proporcionan el fundamento jurídico para esta evaluación.

2.2 Concepto y manifestaciones de la discriminación algorítmica

La discriminación algorítmica se produce cuando un sistema automatizado genera, reproduce o amplifica diferencias de trato que perjudican injustificadamente a determinadas personas o grupos. Estas diferencias pueden originarse en los datos utilizados, en las variables seleccionadas, en las reglas de clasificación o en la forma en que se interpreta el resultado. Wang et al. (2024) distinguen varias manifestaciones, entre ellas sesgos incorporados por agentes algorítmicos, discriminación derivada de la selección de características, discriminación mediante variables sustitutivas y efectos desproporcionados. Por ello, el problema no depende únicamente de una intención discriminatoria, sino también de consecuencias objetivamente desfavorables.

La discriminación algorítmica puede manifestarse mediante criterios explícitos o a través de relaciones indirectas entre variables aparentemente neutrales y características protegidas. Un sistema podría excluir una referencia directa al sexo, origen étnico o condición socioeconómica y utilizar, sin embargo, información estrechamente asociada con esas características. Lendvai y Gosztanyi (2025) señalan que el sesgo algorítmico constituye un problema jurídico porque puede surgir de múltiples fases del desarrollo y utilización de inteligencia artificial. Esta circunstancia dificulta identificar la fuente exacta de la desigualdad y exige analizar conjuntamente datos, diseño, finalidad, resultados y contexto institucional en que funciona el sistema.

En la actuación pública, estas manifestaciones adquieren especial gravedad cuando los sistemas intervienen en acceso a prestaciones, fiscalización, clasificación de riesgos, asignación de recursos o evaluación de solicitudes. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, ninguna persona puede ser discriminada por razones expresamente enumeradas ni por cualquier otra distinción que tenga por objeto o resultado menoscabar derechos. La referencia constitucional al resultado resulta particularmente pertinente frente a algoritmos, porque una diferencia de trato puede producirse sin que exista una instrucción programada expresamente para discriminar. El efecto material también debe ser evaluado jurídicamente.

La discriminación algorítmica puede ser acumulativa cuando una clasificación inicial condiciona decisiones posteriores. Una puntuación desfavorable puede aumentar controles, reducir posibilidades de acceso o situar a una persona dentro de categorías que influyan en futuras actuaciones administrativas. Lütz (2022) explica que los impactos algorítmicos pueden

generar formas directas e indirectas de discriminación, especialmente cuando modelos aparentemente neutrales reproducen patrones históricos de desigualdad. Esta característica impide analizar cada decisión de forma completamente aislada. En sistemas integrados, un resultado previo puede convertirse en dato de entrada para otro procedimiento y consolidar progresivamente una diferencia de trato inicialmente difícil de detectar.

La protección internacional de la igualdad proporciona criterios para evaluar estas manifestaciones. La Convención Americana sobre Derechos Humanos (1969), en su artículo 24, reconoce el derecho de todas las personas a igual protección de la ley, mientras que su artículo 1.1 obliga a garantizar los derechos reconocidos sin discriminación. Del mismo modo, el Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 26, establece igualdad ante la ley y protección efectiva contra la discriminación. Estos mandatos permiten evaluar decisiones algorítmicas atendiendo a sus efectos, porque la tecnología empleada por una institución pública no modifica las obligaciones internacionales asumidas por el Estado.

Tabla 4

Principales manifestaciones de la discriminación algorítmica en la actuación pública

Manifestación	Forma de aparición	Ejemplo en la administración pública	Riesgo jurídico
Sesgo en los datos	Registros históricos reflejan desigualdades previas	Sistema que aprende de decisiones administrativas históricamente desiguales	Reproducción de discriminación existente
Selección de características	Se utilizan variables vinculadas con condiciones protegidas	Priorización basada en variables asociadas indirectamente con origen social	Diferencia injustificada de trato
Discriminación por proxy	Una variable aparentemente neutral sustituye una característica protegida	Código postal utilizado como aproximación al nivel socioeconómico	Discriminación indirecta
Impacto dispar	Una misma regla genera efectos más adversos para un grupo	Algoritmo de elegibilidad con tasas de rechazo significativamente distintas	Afectación de igualdad material
Retroalimentación algorítmica	Resultados anteriores alimentan nuevas decisiones	Mayor control futuro sobre quienes fueron previamente clasificados como riesgo	Consolidación de desigualdades
Error diferencial	El sistema presenta distinta precisión entre grupos	Mayor número de falsos positivos para determinada población	Distribución desigual de cargas

Nota. Las manifestaciones pueden presentarse de manera simultánea y deben evaluarse atendiendo tanto al funcionamiento del sistema como a sus efectos sobre personas y grupos.

La utilización de datos personales puede intensificar estas formas de discriminación cuando la administración combina información procedente de diferentes registros. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige principios de pertinencia, minimización, proporcionalidad y calidad durante el tratamiento. Estos principios impiden asumir que toda información disponible resulta legítimamente utilizable para realizar clasificaciones automatizadas. Además, el artículo 20 reconoce derechos frente a valoraciones automatizadas capaces de producir efectos jurídicos o afectar derechos fundamentales. La relación entre protección de datos e igualdad es directa cuando variables personales determinan probabilidades diferenciadas de acceder a prestaciones, controles o decisiones estatales.

Desde el derecho comparado, el Reglamento (UE) 2024/1689 incorpora medidas destinadas a reducir riesgos discriminatorios en determinados sistemas de inteligencia artificial. Su artículo 10 exige, para sistemas de alto riesgo, prácticas de gobernanza y gestión de datos relacionadas con pertinencia, representatividad y calidad de los conjuntos utilizados. Estas exigencias buscan disminuir errores y sesgos capaces de afectar derechos fundamentales. Aunque esta regulación no constituye derecho ecuatoriano, proporciona un criterio comparativo relevante: la prevención de discriminación debe comenzar antes de que el sistema produzca decisiones. La revisión posterior de casos individuales resulta insuficiente cuando el origen del problema se encuentra incorporado estructuralmente en los datos o modelos.

La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021), en sus párrafos 28 y 29, vincula la equidad y la no discriminación con la obligación de promover justicia social y evitar resultados discriminatorios durante el ciclo de vida de los sistemas de inteligencia artificial. Este enfoque desplaza la atención desde la intención del diseñador hacia las consecuencias de la tecnología. Para la administración pública, ello implica evaluar previamente grupos potencialmente afectados, controlar resultados durante la implementación y modificar el sistema cuando aparezcan patrones injustificados de exclusión. La prevención debe formar parte del diseño institucional y no limitarse a mecanismos de reclamación posteriores.

En consecuencia, la discriminación algorítmica comprende distintas formas de desigualdad generadas o reforzadas mediante sistemas automatizados. Puede originarse en datos históricos, variables de entrada, modelos de clasificación, errores diferenciales o procesos acumulativos que afectan repetidamente a ciertos grupos. Wang et al. (2024) muestran que estas manifestaciones requieren respuestas diferenciadas porque no todas tienen el mismo origen ni pueden corregirse mediante un único mecanismo. La administración debe examinar el sistema

como un proceso completo, desde la recopilación de información hasta la aplicación de sus resultados. Esta perspectiva permite avanzar hacia el análisis específico de los sesgos incorporados en los datos utilizados por sistemas automatizados.

2.3 Sesgos en los datos utilizados por sistemas automatizados

Los sesgos en los datos constituyen una de las principales fuentes de desigualdad en los sistemas automatizados, porque los modelos dependen de la información utilizada para entrenar, validar o ejecutar sus operaciones. Los datos pueden contener errores, ausencias, desequilibrios o patrones históricos asociados con prácticas discriminatorias. Wang et al. (2024) explican que la discriminación algorítmica puede originarse antes del funcionamiento del modelo, especialmente cuando los conjuntos de datos representan de manera insuficiente a determinados grupos o incorporan relaciones socialmente desiguales. Por ello, la calidad de los datos debe analizarse no solo desde precisión técnica, sino también desde sus consecuencias distributivas.

Un primer tipo de sesgo aparece cuando los datos históricos reflejan decisiones públicas tomadas bajo condiciones de desigualdad. Si un sistema aprende de esos registros, puede reproducir patrones anteriores y presentarlos posteriormente como resultados objetivos. Lendvai y Gosztonyi (2025) advierten que el sesgo algorítmico puede originarse en distintas etapas del ciclo de vida de la inteligencia artificial y convertirse en un problema jurídico cuando afecta derechos. La automatización no corrige por sí misma desigualdades contenidas en los datos. Por el contrario, puede reforzarlas mediante aplicaciones repetidas, especialmente cuando la administración utiliza resultados históricos para predecir riesgos, priorizar inspecciones o clasificar personas.

Otro problema surge cuando determinados grupos están subrepresentados en las bases utilizadas por el sistema. Si los datos disponibles describen con mayor precisión a una parte de la población que a otra, el algoritmo puede presentar tasas de error diferentes entre grupos. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021), en su párrafo 28, establece que los actores de inteligencia artificial deben promover la justicia social y proteger la equidad y la no discriminación. Este principio exige que las instituciones públicas identifiquen desequilibrios de representación antes de utilizar datos para decisiones que puedan afectar derechos, oportunidades o acceso a servicios públicos.

El uso de variables sustitutivas constituye otra fuente de sesgo. Una base de datos puede excluir características protegidas expresas y conservar variables que funcionan como indicadores

indirectos de ellas. La zona de residencia, nivel de ingresos, historial de acceso a servicios o determinados patrones administrativos pueden correlacionarse con origen social, condición económica u otras características. Lütz (2022) demuestra que la discriminación algorítmica puede manifestarse mediante impactos indirectos aun cuando el sistema no utilice explícitamente una categoría protegida. Por ello, eliminar determinadas variables sensibles no garantiza neutralidad si otros datos permiten reconstruir, aproximar o reproducir las mismas diferencias entre grupos.

En Ecuador, la calidad de los datos constituye una exigencia jurídica y no únicamente técnica. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora entre sus principios la exactitud, integridad, pertinencia y proporcionalidad del tratamiento. Esto obliga a que los datos utilizados por sistemas automatizados sean adecuados respecto de la finalidad perseguida y no generen decisiones sustentadas en información defectuosa o desactualizada. Asimismo, la Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 1, vincula la organización e interconexión de información pública con seguridad jurídica, eficacia, eficiencia, transparencia y uso de nuevas tecnologías.

Tabla 5

Principales sesgos asociados con los datos utilizados por sistemas automatizados

Tipo de sesgo	Origen	Posible efecto en la administración pública	Medida preventiva
Sesgo histórico	Registros producidos bajo prácticas desiguales	Reproducción de decisiones previamente discriminatorias	Revisar contexto y procedencia de los datos
Subrepresentación	Presencia insuficiente de determinados grupos	Mayor tasa de error para ciertas poblaciones	Evaluar representatividad y cobertura
Sesgo de selección	Datos recopilados de una parte no representativa de la población	Clasificaciones distorsionadas	Revisar criterios de inclusión y exclusión
Variables proxy	Uso de datos asociados indirectamente con características protegidas	Discriminación indirecta	Analizar correlaciones y efectos diferenciados
Datos desactualizados	Información que ya no refleja la situación actual	Decisiones basadas en circunstancias incorrectas	Actualización y rectificación periódica

Tipo de sesgo	Origen	Posible efecto en la administración pública	Medida preventiva
Error de registro	Información incorrecta, incompleta o inconsistente	Falsos positivos o exclusiones injustificadas	Validación, corrección y trazabilidad

Nota. La evaluación del sesgo debe considerar procedencia, representatividad, actualización y relación entre los datos utilizados y los efectos producidos por el sistema.

La legislación ecuatoriana reconoce además mecanismos que permiten corregir información incorrecta antes de que continúe produciendo efectos. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce la acción de hábeas data para conocer la existencia y uso de datos personales, así como solicitar su actualización, rectificación, eliminación o anulación cuando corresponda. Esta garantía adquiere especial relevancia en entornos automatizados, porque un dato erróneo puede alimentar sucesivas decisiones administrativas. El problema deja de limitarse al registro original y puede propagarse cuando distintas instituciones reutilizan o interconectan información para clasificar, evaluar o priorizar a una misma persona.

La gobernanza de datos exige además controlar la representatividad de los conjuntos utilizados por sistemas de alto riesgo. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 10 obligaciones sobre gobernanza y gestión de datos, incluyendo criterios relacionados con pertinencia, representatividad y adecuación respecto de la finalidad prevista. Estas obligaciones responden a la posibilidad de que datos deficientes produzcan sesgos y afectaciones a derechos fundamentales. Aunque este Reglamento no es aplicable como legislación ecuatoriana, muestra que la prevención de discriminación algorítmica debe comenzar en la etapa de preparación de los datos y no únicamente después de que aparezcan resultados perjudiciales.

El control de sesgos requiere igualmente establecer responsabilidades institucionales sobre quién selecciona, depura, integra y actualiza la información. He y Zhang (2025) sostienen que los conflictos jurídicos derivados del poder algorítmico exigen mecanismos de gobernanza capaces de delimitar derechos y responsabilidades. En la administración pública, esta exigencia resulta especialmente importante cuando los datos provienen de múltiples registros. La interoperabilidad no debería implicar una circulación indiscriminada de información. Cada institución debe justificar la pertinencia de los datos utilizados, verificar su calidad y conservar mecanismos para identificar errores, porque la automatización puede amplificar rápidamente las consecuencias de una base defectuosa o de una clasificación incorrecta.

La prevención de sesgos en los datos exige, finalmente, combinar controles técnicos, jurídicos e institucionales. No basta con aumentar el volumen de información si persisten problemas de representación, procedencia o calidad. La UNESCO (2021), en su párrafo 28, vincula explícitamente inteligencia artificial, equidad y no discriminación, mientras que el Reglamento (UE) 2024/1689 exige medidas de gobernanza de datos en sistemas de alto riesgo. Para la administración pública ecuatoriana, estos criterios deben complementarse con las obligaciones de calidad, proporcionalidad y protección de datos previstas en la legislación nacional. El siguiente nivel de análisis corresponde a los sesgos que pueden introducirse directamente durante el diseño y funcionamiento algorítmico.

2.4 Sesgos en el diseño y funcionamiento de los algoritmos

Los sesgos algorítmicos pueden originarse incluso cuando los datos utilizados son técnicamente correctos, porque el diseño del sistema incorpora decisiones humanas sobre objetivos, variables, pesos, umbrales y criterios de clasificación. Lendvai y Gosztonyi (2025) explican que el sesgo puede introducirse en distintas etapas del desarrollo de la inteligencia artificial y convertirse en un problema jurídico cuando genera resultados sistemáticamente desfavorables. La selección de qué resultado debe optimizar el algoritmo nunca es completamente neutral, pues refleja prioridades definidas previamente. En la administración pública, estas decisiones deben examinarse con especial cuidado cuando condicionan acceso a prestaciones, controles, sanciones o cualquier actuación capaz de afectar derechos.

Una fuente importante de sesgo aparece en la definición de la variable objetivo que el sistema intenta predecir o maximizar. Un algoritmo diseñado para identificar riesgo, fraude, vulnerabilidad o prioridad necesita traducir conceptos administrativos complejos en indicadores cuantificables. Wang et al. (2024) muestran que la discriminación algorítmica puede surgir de la selección de características y de decisiones adoptadas durante la construcción del modelo. Si una variable utilizada como aproximación representa de manera incompleta el fenómeno real, el sistema puede clasificar incorrectamente a determinadas personas. El diseño debe justificar, por tanto, la relación entre cada indicador utilizado y la finalidad jurídica del procedimiento administrativo correspondiente.

Los umbrales de decisión también pueden producir efectos diferenciados. Un sistema puede asignar puntuaciones continuas y posteriormente convertirlas en categorías como riesgo alto, elegible, prioritario o sujeto a revisión. La ubicación del punto de corte determina quién recibe una consecuencia administrativa y quién queda fuera de ella. He y Zhang (2025) señalan que

el poder algorítmico genera conflictos jurídicos cuando los mecanismos tecnológicos condicionan derechos y distribuyen cargas sin controles suficientes. Esta circunstancia exige que la administración pueda explicar por qué adoptó determinados umbrales y demostrar que estos guardan relación razonable con la finalidad pública perseguida, especialmente cuando producen efectos restrictivos.

La elección de métricas de precisión constituye otro componente susceptible de introducir desigualdad. Un sistema puede presentar buen rendimiento global y, al mismo tiempo, equivocarse con mayor frecuencia respecto de determinados grupos. La precisión promedio puede ocultar falsos positivos o falsos negativos distribuidos de manera desigual. El Reglamento (UE) 2024/1689, utilizado aquí como referencia comparada, establece en su artículo 15 que los sistemas de inteligencia artificial de alto riesgo deben alcanzar niveles adecuados de precisión, robustez y ciberseguridad durante su ciclo de vida. Esta exigencia muestra que evaluar funcionamiento implica examinar la fiabilidad efectiva del sistema y no limitarse a constatar que produce resultados técnicamente operativos.

El sesgo también puede surgir durante la configuración de modelos que utilizan variables relacionadas indirectamente con características protegidas. Una combinación de información territorial, económica, educativa o laboral puede permitir al algoritmo reconstruir diferencias asociadas con género, origen social u otras condiciones, aunque estas no se incorporen expresamente. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, ninguna persona puede ser discriminada por las categorías allí enumeradas ni por cualquier otra distinción cuyo objeto o resultado menoscabe derechos. Esta formulación resulta especialmente pertinente porque permite valorar el efecto producido y no únicamente la intención incorporada en el diseño.

Los procesos de aprendizaje automático añaden complejidad cuando el funcionamiento del modelo se modifica mediante nuevas observaciones o mecanismos de retroalimentación. Una clasificación inicial puede influir en los datos recopilados posteriormente y reforzar el mismo patrón que la originó. Teo (2025) advierte que determinados impactos de la inteligencia artificial sobre los derechos pueden acumularse progresivamente y resultar menos visibles cuando se examinan decisiones aisladas. En el sector público, este fenómeno puede producirse si grupos clasificados inicialmente como de mayor riesgo reciben controles más frecuentes, generando nuevos registros que posteriormente confirman artificialmente la clasificación original. La supervisión debe considerar estas dinámicas de retroalimentación institucional.

Figura 3

Sesgos en el diseño y funcionamiento de los algoritmos



Nota. El esquema presenta las principales fuentes de sesgo algorítmico asociadas con las decisiones de diseño, los umbrales, las métricas, las variables indirectas y los procesos de retroalimentación que pueden generar resultados desiguales.

La responsabilidad sobre el diseño tampoco puede trasladarse completamente a proveedores tecnológicos externos. Aunque una administración adquiera un sistema desarrollado por una empresa, conserva la obligación de comprobar su adecuación a las competencias, finalidades y derechos involucrados. El Código Orgánico Administrativo (2017), en su artículo 14, somete la actuación administrativa al principio de juridicidad, por lo que la utilización de una herramienta privada no puede introducir criterios incompatibles con el ordenamiento jurídico. De manera complementaria, Dragomir et al. (2026) destacan la importancia de una gobernanza de inteligencia artificial centrada en derechos fundamentales y responsabilidad institucional. La contratación tecnológica no elimina la obligación pública de supervisar su funcionamiento. La transparencia del diseño resulta igualmente relevante porque ciertos sesgos solo pueden identificarse cuando existe información suficiente sobre variables, criterios, límites y desempeño del sistema. Freitas (2026) analiza la relación entre regulación de inteligencia artificial, protección de datos y derechos civiles, destacando la necesidad de controles jurídicos frente a herramientas capaces de afectar posiciones individuales. Desde la perspectiva ecuatoriana, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce garantías frente a decisiones basadas total o parcialmente en valoraciones

automatizadas. La posibilidad de solicitar explicación y cuestionar el resultado pierde eficacia si la administración desconoce cómo fue configurado el sistema utilizado.

La prevención de sesgos debe incorporarse desde el diseño y continuar durante todo el funcionamiento del algoritmo. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 10, exige que las partes adopten o mantengan medidas destinadas a garantizar igualdad y no discriminación en las actividades desarrolladas durante el ciclo de vida de los sistemas de inteligencia artificial. Este enfoque resulta relevante porque desplaza la atención desde la corrección posterior hacia la prevención estructural. Las pruebas previas, evaluaciones periódicas y análisis de resultados diferenciados permiten detectar problemas antes de que se consoliden como prácticas administrativas sistemáticas.

La evaluación del funcionamiento debe incluir además mecanismos para detectar desviaciones entre el comportamiento esperado y los resultados reales. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) vincula equidad, no discriminación, responsabilidad y supervisión durante todo el ciclo de vida de estos sistemas. Esta perspectiva exige observar cómo funciona la herramienta después de su implementación, porque un modelo inicialmente aceptable puede generar efectos distintos cuando cambian los datos, la población o las condiciones institucionales. La auditoría periódica permite identificar tasas desiguales de error, variaciones injustificadas en resultados y efectos acumulativos que no fueron detectados durante las pruebas iniciales.

Los sesgos en el diseño y funcionamiento de los algoritmos muestran que la discriminación no puede atribuirse únicamente a datos defectuosos. Las decisiones sobre objetivos, variables, umbrales, métricas, arquitectura y mecanismos de actualización condicionan la distribución posterior de beneficios y cargas. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, obliga a evitar resultados discriminatorios, mientras que el Consejo de Europa (2024), en su artículo 10, sitúa igualdad y no discriminación dentro de las obligaciones vinculadas al ciclo de vida de la inteligencia artificial. El análisis debe avanzar ahora hacia los grupos que pueden experimentar de manera especialmente intensa estos efectos.

2.5 Impacto diferenciado de las decisiones automatizadas en grupos vulnerables

Las decisiones automatizadas pueden producir efectos diferenciados cuando los sistemas utilizan datos, criterios o modelos que no representan adecuadamente las condiciones de determinados grupos. La vulnerabilidad no deriva únicamente de características individuales,

sino también de contextos sociales, económicos, territoriales o institucionales que pueden intensificar las consecuencias de una decisión pública. Teo (2025) advierte que los impactos de la inteligencia artificial sobre los derechos humanos pueden acumularse progresivamente y afectar de manera desigual a quienes cuentan con menores posibilidades de cuestionar los resultados. En la administración pública, estas diferencias resultan relevantes cuando la automatización condiciona prestaciones, controles, servicios o reconocimiento de derechos.

La Constitución de la República del Ecuador (2008), en su artículo 35, establece atención prioritaria para personas adultas mayores, niñas, niños y adolescentes, mujeres embarazadas, personas con discapacidad, personas privadas de libertad y quienes padezcan enfermedades catastróficas o de alta complejidad. Este mandato adquiere importancia cuando sistemas automatizados intervienen en servicios dirigidos a estas poblaciones. Una herramienta diseñada bajo condiciones generales puede generar barreras particulares si no considera necesidades específicas de accesibilidad, comunicación o protección reforzada. La igualdad administrativa exige, por tanto, valorar anticipadamente si la tecnología incrementa dificultades existentes o limita el acceso efectivo a prestaciones y procedimientos estatales.

Las personas con discapacidad pueden experimentar impactos particulares cuando las interfaces, sistemas de identificación o mecanismos automatizados no consideran diversidad funcional. El artículo 47 de la Constitución de la República del Ecuador (2008) reconoce derechos y medidas específicas destinadas a garantizar inclusión y equiparación de oportunidades de las personas con discapacidad. En entornos automatizados, esta obligación implica evitar diseños que excluyan a quienes requieren formatos accesibles, asistencia o vías alternativas de interacción con la administración. La innovación tecnológica no puede convertirse en una condición adicional para ejercer derechos. Si un sistema automatizado restringe materialmente la participación de ciertas personas, la administración debe establecer ajustes y mecanismos complementarios adecuados.

El impacto diferenciado también puede observarse en relación con el género. Lütz (2022) explica que los algoritmos pueden producir discriminación directa o indirecta cuando utilizan información histórica, variables sustitutivas o criterios que afectan de manera desproporcionada a determinados grupos. En Ecuador, el artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) prohíbe la discriminación por sexo, identidad de género y otras condiciones personales o sociales. Esta prohibición obliga a evaluar si un sistema empleado para asignar beneficios, seleccionar personas, priorizar servicios o

determinar riesgos genera diferencias sistemáticas que no puedan justificarse mediante una finalidad legítima y proporcional.

Las condiciones socioeconómicas también pueden transformarse en factores de desigualdad algorítmica. Wang et al. (2024) señalan que variables aparentemente neutrales pueden funcionar como aproximaciones de características protegidas o condiciones sociales y generar impactos adversos. En la administración pública, información sobre residencia, historial laboral, ingresos o acceso previo a servicios puede influir en clasificaciones automatizadas y afectar especialmente a poblaciones con menores recursos. El artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) incluye la condición socioeconómica entre los motivos respecto de los cuales se prohíbe la discriminación. Esta protección exige examinar también variables indirectamente relacionadas con dicha condición.

La protección internacional refuerza estas obligaciones. La Convención Americana sobre Derechos Humanos (1969), en su artículo 24, reconoce la igualdad ante la ley, mientras que su artículo 1.1 exige respetar y garantizar los derechos sin discriminación. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 26, reconoce igualmente la igualdad y la protección efectiva frente a cualquier discriminación. Aplicados a sistemas automatizados, estos estándares obligan a considerar resultados concretos y no únicamente reglas formales. Una decisión tecnológicamente uniforme puede resultar jurídicamente problemática cuando impone mayores cargas, errores o exclusiones sobre ciertos grupos sin una justificación objetiva, razonable y compatible con los derechos humanos.

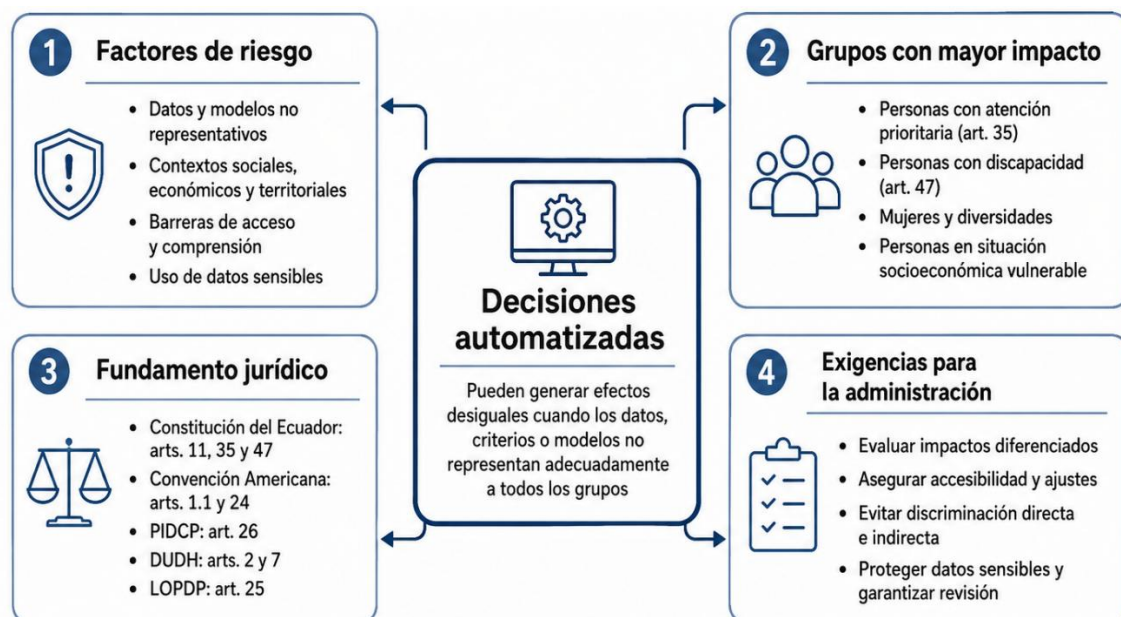
La Declaración Universal de Derechos Humanos (1948), en sus artículos 2 y 7, reconoce respectivamente el disfrute de derechos sin distinción y la igualdad ante la ley con protección frente a la discriminación. Estos principios permiten interpretar la automatización administrativa desde una perspectiva centrada en la persona. El riesgo aparece cuando quienes poseen menos recursos tecnológicos, menor alfabetización digital o mayores dificultades para relacionarse con instituciones públicas encuentran obstáculos adicionales para comprender o impugnar decisiones automatizadas. La transformación digital debe evitar que la capacidad para utilizar plataformas, interpretar resultados o acceder a asistencia se convierta en un factor que condicione materialmente el ejercicio de derechos.

La protección de datos adquiere especial relevancia cuando la vulnerabilidad se relaciona con información sensible. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 25, identifica categorías especiales de datos personales, entre ellas datos sensibles y

datos relativos a salud. El uso automatizado de esta información requiere mayores precauciones porque puede producir clasificaciones que incidan sobre derechos o servicios. Freitas (2026) analiza la relación entre regulación de inteligencia artificial, protección de datos y derechos civiles, evidenciando que los riesgos regulatorios aumentan cuando sistemas automatizados operan sobre información capaz de revelar condiciones particularmente protegidas de las personas.

Figura 4

Impacto diferenciado de las decisiones automatizadas en grupos vulnerables



Nota. El esquema sintetiza los principales factores de riesgo, grupos con mayor exposición, fundamentos jurídicos y exigencias institucionales para prevenir efectos discriminatorios derivados de decisiones públicas automatizadas.

La administración también debe considerar que un mismo sistema puede producir tasas de error diferentes entre grupos. Una herramienta con precisión general elevada puede generar más falsos positivos o falsos negativos para poblaciones con menor representación en los datos. El Reglamento (UE) 2024/1689, como referencia comparada, establece en su artículo 10 exigencias de gobernanza de datos para sistemas de alto riesgo y, en su artículo 15, obligaciones relacionadas con precisión y robustez. Estas disposiciones muestran que la evaluación debe desagregar resultados y comprobar si determinados grupos soportan una proporción mayor de errores. La igualdad requiere analizar cómo se distribuyen las fallas del sistema, no solo su rendimiento promedio.

La prevención del impacto diferenciado exige incorporar evaluaciones previas y controles durante todo el ciclo de vida de la tecnología. La Recomendación sobre la Ética de la

Inteligencia Artificial de la UNESCO (2021), particularmente en sus párrafos 28 y 29, relaciona equidad, inclusión y no discriminación con el desarrollo y utilización de sistemas de inteligencia artificial. Asimismo, Dragomir et al. (2026) destacan la necesidad de una gobernanza centrada en derechos fundamentales y responsabilidad institucional. En el sector público, esto implica identificar poblaciones potencialmente afectadas, analizar consecuencias diferenciadas, establecer indicadores de seguimiento y modificar sistemas cuando se detecten patrones persistentes de exclusión o desventaja.

El impacto diferenciado sobre grupos vulnerables obliga, finalmente, a superar una concepción exclusivamente formal de igualdad. La administración debe analizar quiénes resultan afectados, con qué intensidad, mediante qué mecanismos y qué posibilidades tienen de cuestionar el resultado. El artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) exige igualdad y prohíbe discriminaciones cuyo objeto o resultado menoscabe derechos, mientras que el artículo 35 establece protección prioritaria para determinados grupos. La automatización pública será compatible con estas obligaciones cuando incorpore mecanismos que permitan detectar desigualdades, adaptar procedimientos y evitar que las ventajas tecnológicas se obtengan trasladando riesgos desproporcionados a poblaciones en situación de mayor vulnerabilidad.

2.6 Discriminación directa, indirecta y algorítmica

La discriminación directa se produce cuando una persona recibe un trato desfavorable basado explícitamente en una característica protegida, como sexo, edad, discapacidad, origen étnico o condición socioeconómica. En sistemas automatizados, esta forma puede aparecer cuando una variable protegida interviene de manera expresa en la clasificación o decisión. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, prohíbe distinciones que tengan por objeto o resultado menoscabar derechos. Este mandato resulta aplicable a las decisiones algorítmicas, pues una entidad pública no puede incorporar criterios discriminatorios dentro de un sistema y justificar posteriormente el resultado mediante su carácter tecnológico.

La discriminación indirecta presenta mayor complejidad porque puede surgir de criterios aparentemente neutrales que generan efectos desproporcionados sobre determinados grupos. Lütz (2022) explica que los algoritmos pueden producir impactos indirectos cuando utilizan variables que, sin mencionar expresamente una característica protegida, mantienen una estrecha relación con ella. En la administración pública, esto puede ocurrir cuando residencia,

ingresos, historial laboral o patrones de utilización de servicios funcionan como sustitutos de condiciones socioeconómicas o personales. La ausencia de una clasificación explícita basada en sexo, origen o discapacidad no elimina el problema jurídico si el resultado perjudica sistemáticamente a un grupo sin justificación suficiente.

La discriminación algorítmica comprende situaciones en las que sistemas automatizados generan, reproducen o amplifican desigualdades durante la recopilación de datos, construcción del modelo, clasificación o aplicación de resultados. Wang et al. (2024) identifican mecanismos relacionados con selección de características, variables proxy, sesgos incorporados y efectos adversos diferenciados. Esta categoría permite comprender que la discriminación puede resultar de varias etapas conectadas y no únicamente de una regla explícita. El análisis jurídico debe reconstruir el proceso completo, identificar dónde surge la diferencia y determinar si existe una justificación legítima. La complejidad tecnológica no reduce la obligación institucional de responder por los resultados producidos.

Las tres formas pueden coexistir dentro de un mismo sistema. Un algoritmo puede incluir una característica protegida de forma directa, utilizar variables asociadas indirectamente con ella y, además, aprender patrones discriminatorios contenidos en datos históricos. Lendvai y Gosztonyi (2025) señalan que el sesgo algorítmico puede surgir en distintas fases del ciclo de vida de la inteligencia artificial y requiere respuestas jurídicas diferenciadas. Por ello, clasificar una afectación únicamente como directa o indirecta puede resultar insuficiente cuando intervienen mecanismos computacionales complejos. La discriminación algorítmica funciona como una categoría analítica que permite observar cómo diferentes fuentes de desigualdad interactúan dentro del mismo procedimiento automatizado.

El derecho internacional obliga a examinar estas diferencias desde sus efectos sobre la igualdad. La Convención Americana sobre Derechos Humanos (1969), en su artículo 1.1, exige garantizar los derechos reconocidos sin discriminación, mientras que su artículo 24 establece la igualdad ante la ley y el derecho a igual protección. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 26, reconoce igualmente la igualdad ante la ley y la protección contra cualquier discriminación. Estos estándares no dependen de que la diferencia haya sido producida por una persona o un algoritmo, sino del efecto que la actuación estatal tiene sobre los derechos de quienes resultan afectados.

Tabla 6

Diferencias entre discriminación directa, indirecta y algorítmica

Tipo de discriminación	Característica principal	Manifestación en sistemas automatizados	Ejemplo administrativo	Criterio jurídico de evaluación
Directa	Utiliza expresamente una característica protegida	El sistema clasifica de forma distinta según sexo, edad, discapacidad u otra condición	Rechazo automático basado directamente en una categoría protegida	Existencia de trato diferenciado expresamente asociado con una condición protegida
Indirecta	Regla aparentemente neutral con efectos desproporcionados	Variables neutrales afectan especialmente a un grupo	Zona de residencia utilizada como criterio que perjudica sistemáticamente a una población	Impacto diferenciado y justificación objetiva y proporcional
Algorítmica por datos	El sesgo procede de información histórica o no representativa	El modelo aprende desigualdades existentes	Predicción basada en decisiones administrativas históricamente sesgadas	Calidad, representatividad y pertinencia de los datos
Algorítmica por diseño	El sesgo deriva de variables, pesos, objetivos o umbrales	El sistema distribuye errores o cargas de manera desigual	Umbral de riesgo que aumenta falsos positivos en un grupo	Diseño, necesidad, proporcionalidad y efectos
Algorítmica acumulativa	Diferentes decisiones automatizadas refuerzan una desventaja	Resultados previos alimentan nuevas clasificaciones	Mayor vigilancia futura por una clasificación algorítmica anterior	Evaluación del ciclo completo y efectos acumulados

Nota. La discriminación algorítmica puede incorporar elementos de discriminación directa e indirecta; su identificación exige analizar datos, diseño, funcionamiento y efectos de la decisión.

La igualdad ante la ley exige valorar especialmente las consecuencias materiales de las decisiones automatizadas. El artículo 26 del Pacto Internacional de Derechos Civiles y Políticos (1966) reconoce a todas las personas igual protección legal sin discriminación, mientras que el artículo 24 de la Convención Americana sobre Derechos Humanos (1969) establece la misma garantía en el sistema interamericano. Estos mandatos resultan relevantes frente a sistemas cuyos efectos son difíciles de detectar individualmente. Una diferencia estadística persistente entre grupos puede revelar un problema estructural, aunque cada decisión aislada parezca formalmente neutral. La administración debe evaluar patrones colectivos además de revisar reclamaciones individuales.

La prevención de discriminación algorítmica también requiere controles sobre los datos y el diseño. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 10 obligaciones de gobernanza de datos para determinados sistemas de alto riesgo, incluyendo criterios relacionados con calidad y representatividad de los conjuntos utilizados. Estas exigencias responden a la posibilidad de que información defectuosa o no representativa produzca resultados discriminatorios. Aunque esta disposición no constituye derecho aplicable directamente en Ecuador, muestra que la protección de la igualdad debe incorporarse antes de la implementación. La revisión posterior resulta insuficiente cuando el sesgo está integrado estructuralmente en el modelo automatizado.

La administración pública debe considerar además que igualdad matemática e igualdad jurídica no son conceptos equivalentes. He y Zhang (2025) analizan los conflictos de derechos asociados con el poder algorítmico y la necesidad de respuestas regulatorias capaces de limitar sus efectos. Un modelo puede distribuir determinadas tasas de error de manera estadísticamente equilibrada y aun así aplicar criterios jurídicamente improcedentes. La evaluación debe examinar finalidad, necesidad, proporcionalidad y consecuencias concretas. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 4, reconoce el derecho a la igualdad formal, igualdad material y no discriminación, lo que exige considerar también las condiciones reales de las personas.

Distinguir discriminación directa, indirecta y algorítmica permite identificar con mayor precisión dónde se produce una desigualdad y qué medida correctiva resulta adecuada. La discriminación directa exige eliminar criterios expresamente prohibidos; la indirecta requiere revisar reglas neutrales con efectos desproporcionados; y la algorítmica demanda examinar datos, diseño, funcionamiento y resultados acumulativos. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) sitúa la equidad y la no discriminación entre los principios que deben orientar el ciclo de vida de los sistemas de inteligencia artificial. Este enfoque proporciona la base para avanzar hacia mecanismos preventivos capaces de identificar impactos discriminatorios antes de consolidarse.

2.7 Evaluación y prevención de impactos discriminatorios

La evaluación de impactos discriminatorios debe realizarse antes de implementar un sistema automatizado y continuar durante todo su ciclo de funcionamiento. Su finalidad consiste en identificar si los datos, variables, criterios de clasificación o resultados pueden generar diferencias injustificadas entre personas o grupos. Wang et al. (2024) muestran que la

discriminación algorítmica puede surgir mediante mecanismos diversos, incluidos sesgos de datos, variables proxy y efectos adversos diferenciados. Por ello, una administración no debería limitarse a comprobar la precisión general del sistema, sino examinar cómo se distribuyen errores, beneficios y cargas entre grupos potencialmente afectados por una decisión automatizada.

La evaluación debe partir del principio constitucional de igualdad. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, prohíbe toda discriminación cuyo objeto o resultado menoscabe o anule derechos y establece que el Estado debe adoptar medidas de acción afirmativa en favor de quienes se encuentren en situación de desigualdad. Este mandato obliga a evaluar no solo reglas expresamente discriminatorias, sino también efectos diferenciados derivados de criterios aparentemente neutrales. Cuando un sistema automatizado produce tasas significativamente distintas de rechazo, fiscalización, priorización o error entre grupos, la administración debe determinar las causas y justificar jurídicamente cualquier diferencia de trato.

La evaluación preventiva requiere revisar la información que alimenta el sistema. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece principios de finalidad, pertinencia, minimización, proporcionalidad, calidad y transparencia en el tratamiento de datos personales. Estos principios permiten cuestionar conjuntos de datos incompletos, desactualizados o excesivos antes de que sean utilizados para clasificaciones automatizadas. Thomaidou y Limniotis (2025) relacionan la protección de datos con las evaluaciones de impacto sobre derechos fundamentales, mostrando que ambos mecanismos pueden complementarse cuando la inteligencia artificial procesa información personal. La prevención comienza, por tanto, desde la selección y gobernanza de los datos.

La evaluación tampoco debe limitarse a la fase de diseño, porque los efectos del sistema pueden variar después de su implementación. Lendvai y Gosztanyi (2025) explican que el sesgo algorítmico puede introducirse o manifestarse en diferentes etapas del ciclo de vida de la inteligencia artificial. Esto exige supervisar tasas de error, resultados desagregados, reclamaciones y cambios en la población sobre la cual opera el sistema. La administración debe establecer indicadores que permitan detectar desviaciones y revisar periódicamente si el modelo continúa siendo adecuado para la finalidad prevista. La ausencia de reclamaciones no demuestra necesariamente ausencia de discriminación, especialmente cuando las personas desconocen la automatización.

La prevención de impactos discriminatorios también exige identificar anticipadamente los derechos que pueden resultar afectados. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 16, exige medidas para identificar, evaluar, prevenir y mitigar riesgos considerando impactos reales y potenciales sobre derechos humanos, democracia y Estado de derecho. La disposición contempla además documentación de riesgos y, cuando corresponda, pruebas antes del primer uso o después de modificaciones significativas. Aunque su aplicabilidad depende de la condición jurídica de cada Estado parte, constituye un estándar internacional útil para estructurar evaluaciones preventivas de sistemas públicos.

Tabla 7

Elementos para evaluar y prevenir impactos discriminatorios en sistemas automatizados

Etapas de evaluación	Aspecto que debe examinarse	Riesgo discriminatorio	Medida preventiva
Definición de finalidad	Objetivo y necesidad del sistema	Uso de automatización sin justificación suficiente	Determinar finalidad legítima y proporcionalidad
Selección de datos	Calidad, actualidad y representatividad	Subrepresentación o reproducción de desigualdades históricas	Depurar, actualizar y evaluar cobertura
Diseño del modelo	Variables, pesos, umbrales y métricas	Uso de proxies o distribución desigual de errores	Analizar variables y resultados por grupos
Pruebas previas	Rendimiento general y diferenciado	Detección tardía de efectos adversos	Realizar pruebas antes de la implementación
Implementación	Forma de utilización del resultado	Dependencia excesiva del sistema	Establecer supervisión humana efectiva
Seguimiento	Resultados reales y reclamaciones	Aparición progresiva de patrones discriminatorios	Auditorías y monitoreo periódico
Corrección	Respuesta frente a impactos identificados	Persistencia del daño	Modificar, suspender o retirar el sistema

Nota. La evaluación debe abarcar el ciclo de vida completo del sistema y considerar tanto riesgos previsibles como efectos discriminatorios detectados durante su utilización.

La evaluación de impacto sobre derechos fundamentales ofrece un mecanismo más amplio para incorporar la igualdad dentro de la gobernanza algorítmica. Como referencia comparada, el artículo 27 del Reglamento (UE) 2024/1689 exige, para determinados responsables públicos o prestadores de servicios públicos que utilizan sistemas de inteligencia artificial de alto riesgo, una evaluación previa de sus efectos sobre derechos fundamentales. Esta evaluación debe atender al contexto de uso y a los grupos que pueden resultar afectados. Aunque esta obligación

pertenece al ordenamiento de la Unión Europea, proporciona un criterio útil para las administraciones públicas: identificar consecuencias sobre derechos antes de convertir un sistema automatizado en parte ordinaria del procedimiento institucional.

La prevención debe incorporar además mecanismos de participación y conocimiento institucional. Dragomir et al. (2026) vinculan la gobernanza de inteligencia artificial centrada en las personas con responsabilidad, derechos fundamentales y capacidad institucional. Una evaluación exclusivamente técnica realizada por desarrolladores puede pasar por alto implicaciones jurídicas o sociales relevantes. Por ello, los equipos responsables deberían integrar conocimientos jurídicos, administrativos, técnicos y de protección de datos, además de considerar información sobre poblaciones potencialmente afectadas. La diversidad de perspectivas facilita detectar variables problemáticas, supuestos incorrectos o barreras que no aparecen en pruebas puramente computacionales y permite fundamentar mejor la decisión de implementar, modificar o rechazar una herramienta.

Las medidas preventivas deben ser proporcionales al nivel de riesgo. Un sistema utilizado únicamente para ordenar documentos internos no requiere el mismo grado de control que otro destinado a determinar elegibilidad para prestaciones, riesgo de fraude o acceso a servicios esenciales. El Consejo de Europa (2024), en su artículo 16, establece un enfoque diferenciado para la gestión de riesgos e impactos, considerando el contexto y el uso previsto del sistema. Esta lógica permite concentrar controles más exigentes donde la posible afectación de derechos sea mayor. La prevención efectiva exige, por tanto, relacionar intensidad de supervisión, capacidad de daño y relevancia jurídica de la decisión automatizada.

La evaluación y prevención de impactos discriminatorios debe concluir en decisiones institucionales concretas. Si las pruebas muestran diferencias persistentes e injustificadas, la respuesta no puede limitarse a documentarlas. La administración debe modificar datos, variables, umbrales o procedimientos y, cuando el riesgo no pueda reducirse razonablemente, suspender o descartar el sistema. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) vincula equidad y no discriminación con la gobernanza responsable de la inteligencia artificial, mientras que el artículo 11, numeral 2, de la Constitución ecuatoriana exige impedir resultados discriminatorios. La evaluación cumple su función cuando permite prevenir daños antes de que se conviertan en prácticas administrativas repetidas.

2.8 Obligaciones de la administración pública frente a la igualdad algorítmica

La administración pública tiene la obligación de garantizar que los sistemas automatizados utilizados en sus procedimientos respeten el principio de igualdad y no produzcan discriminaciones injustificadas. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 2, establece que todas las personas son iguales y prohíbe toda discriminación cuyo objeto o resultado menoscabe derechos. Este mandato vincula también las decisiones apoyadas por algoritmos, aunque la diferencia de trato no haya sido programada expresamente. Por ello, las instituciones deben evaluar tanto las reglas incorporadas al sistema como sus efectos reales sobre personas y grupos potencialmente afectados.

La obligación administrativa comienza antes de la implementación del sistema. Las entidades públicas deben examinar la finalidad perseguida, la pertinencia de automatizar el procedimiento y los posibles efectos diferenciados. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 10, incorpora la igualdad y la no discriminación entre los principios aplicables durante el ciclo de vida de los sistemas de inteligencia artificial. Aunque su aplicación depende de la vinculación jurídica correspondiente, constituye un estándar relevante para evaluar tecnologías públicas. La igualdad debe integrarse desde el diseño y no limitarse a corregir daños posteriores.

Una segunda obligación consiste en controlar la calidad y pertinencia de los datos utilizados. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece principios aplicables al tratamiento, entre ellos juridicidad, transparencia, finalidad, pertinencia, minimización, proporcionalidad y calidad. Estos principios obligan a revisar si los datos empleados para clasificar o evaluar personas resultan adecuados para la finalidad administrativa. El uso de información desactualizada, incompleta o desproporcionada puede producir diferencias de trato injustificadas. Por tanto, la administración debe establecer procedimientos de depuración, actualización y revisión antes de incorporar bases de datos en sistemas automatizados.

También existe una obligación de supervisar el funcionamiento efectivo del sistema después de su implementación. Lendvai y Gosztanyi (2025) explican que el sesgo algorítmico puede aparecer en diferentes etapas del ciclo de vida de la inteligencia artificial, por lo que una evaluación inicial no garantiza que el sistema permanezca libre de efectos discriminatorios. La administración debe analizar periódicamente tasas de error, resultados desagregados, reclamaciones y posibles diferencias entre grupos. Esta supervisión debe permitir modificar variables, umbrales o procedimientos cuando se identifiquen patrones injustificados. La

igualdad algorítmica exige control continuo porque los efectos pueden cambiar conforme evolucionan los datos y las condiciones sociales.

La administración tiene además la obligación de evitar que la complejidad tecnológica impida identificar responsabilidades. El Código Orgánico Administrativo (2017), en su artículo 14, somete toda actuación administrativa a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. En consecuencia, un algoritmo no puede operar como fuente autónoma de autoridad ni justificar decisiones incompatibles con el ordenamiento jurídico. La institución que decide incorporar un sistema conserva responsabilidad sobre su selección, configuración y utilización. Si el resultado genera una diferencia de trato injustificada, la explicación de que fue producido automáticamente no excluye la obligación administrativa de revisar y corregir la actuación correspondiente.

La transparencia constituye otra obligación vinculada con la igualdad algorítmica. La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) tiene por objeto garantizar y regular el derecho de acceso a la información pública y obliga a los sujetos públicos a facilitar información bajo los parámetros establecidos por la ley. En contextos automatizados, esta exigencia adquiere relevancia cuando las personas necesitan conocer que una herramienta intervino en el procedimiento, cuáles fueron sus funciones y qué criterios generales influyeron en el resultado. Sin información suficiente, resulta difícil detectar patrones discriminatorios y ejercer mecanismos de control sobre actuaciones que afectan derechos.

La obligación de protección también comprende los registros públicos utilizados para alimentar sistemas automatizados. La Ley del Sistema Nacional de Registro de Datos Públicos (2010) regula la organización, sistematización e interconexión de información proveniente de registros públicos. Su artículo 10 establece reglas sobre precedencia de los datos registrados, lo que evidencia la relevancia jurídica de mantener información coherente y actualizada. En decisiones automatizadas, una inconsistencia registral puede convertirse en una clasificación errónea y afectar de manera reiterada a una persona. La administración debe asegurar, por tanto, mecanismos que permitan detectar, corregir y actualizar información antes de que sea reutilizada en nuevos procedimientos.

La igualdad algorítmica exige asimismo mecanismos efectivos de reclamación y reparación. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho a la tutela efectiva, mientras que su artículo 92 garantiza la acción de hábeas data para conocer, actualizar, rectificar, eliminar o anular datos personales cuando corresponda. Estas garantías

pueden resultar relevantes cuando una decisión automatizada se sustenta en información incorrecta o genera una afectación discriminatoria. A ello se suma la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), que desarrolla las garantías constitucionales destinadas a proteger derechos frente a actuaciones u omisiones públicas contrarias al orden constitucional.

La administración debe garantizar además que la supervisión humana sea real y no meramente formal. Green (2022) advierte que la exigencia de participación humana puede resultar insuficiente cuando el funcionario se limita a validar la recomendación del sistema. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 14 obligaciones de supervisión humana para sistemas de alto riesgo, precisamente para reducir riesgos sobre derechos fundamentales. Esta supervisión debe permitir comprender las limitaciones del sistema, detectar resultados anómalos y apartarse de ellos cuando existan razones justificadas. La igualdad requiere capacidad institucional para cuestionar una recomendación automatizada antes de convertirla en decisión pública.

La prevención de discriminación también exige considerar los derechos humanos como marco de evaluación general. La Declaración Universal de Derechos Humanos (1948), en sus artículos 2 y 7, reconoce el disfrute de derechos sin discriminación y la igualdad ante la ley. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 26, garantiza igual protección legal, mientras que la Convención Americana sobre Derechos Humanos (1969), en sus artículos 1.1 y 24, impone obligaciones de no discriminación e igualdad ante la ley. Estos estándares obligan a valorar las consecuencias de la automatización desde la posición de las personas afectadas y no únicamente desde su rendimiento técnico.

En conjunto, las obligaciones de la administración frente a la igualdad algorítmica abarcan prevención, evaluación, transparencia, supervisión, revisión y reparación. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) vincula expresamente la inteligencia artificial con equidad, inclusión y no discriminación, mientras que Dragomir et al. (2026) destacan la necesidad de una gobernanza pública centrada en derechos fundamentales y responsabilidad institucional. La administración debe demostrar que conoce cómo funciona el sistema, qué efectos produce y qué medidas adopta para corregir desigualdades. La igualdad algorítmica exige una gestión institucional permanente y no una simple declaración de neutralidad tecnológica.

Capítulo 3

Privacidad y protección de datos personales

Frank Eduardo Vargas Iza



3.1 Privacidad y protección de datos como derechos fundamentales

La privacidad y la protección de datos personales constituyen derechos fundamentales que adquieren especial relevancia cuando la administración pública utiliza sistemas automatizados para recopilar, analizar o intercambiar información sobre las personas. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce expresamente el derecho a la protección de datos personales, incluyendo el acceso, la decisión sobre la información y su correspondiente protección. Este reconocimiento impide considerar los datos ciudadanos como simples recursos administrativos disponibles sin restricciones. Toda utilización tecnológica debe mantener la capacidad de la persona para conocer y controlar, dentro del marco jurídico aplicable, el tratamiento de su información.

La protección de datos se relaciona con la privacidad, aunque ambas categorías no son idénticas. La privacidad protege ámbitos de la vida personal frente a interferencias arbitrarias o abusivas, mientras que la protección de datos establece garantías respecto de la recopilación, utilización, conservación, comunicación y demás formas de tratamiento de información personal. La Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege la honra, la dignidad y la vida privada frente a injerencias arbitrarias o abusivas. En contextos automatizados, esta garantía adquiere una dimensión informacional, porque el procesamiento masivo de datos puede permitir inferir comportamientos, relaciones, preferencias o condiciones personales.

El sistema universal de derechos humanos proporciona un fundamento adicional para proteger la privacidad frente al procesamiento tecnológico. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe las interferencias arbitrarias o ilegales en la vida privada, familia, domicilio o correspondencia y reconoce protección legal frente a estas injerencias. Esta disposición mantiene su relevancia cuando las interferencias no provienen de vigilancia física, sino del análisis automatizado de información. La capacidad estatal de combinar registros, detectar patrones o elaborar inferencias sobre una persona debe someterse a criterios jurídicos que impidan tratamientos arbitrarios, desproporcionados o desconectados de una finalidad legítima.

La Declaración Universal de Derechos Humanos (1948), en su artículo 12, establece que nadie debe ser objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia y reconoce el derecho a protección jurídica frente a tales actuaciones. Este principio antecede a las tecnologías actuales, pero conserva plena utilidad para interpretar los

riesgos derivados de la administración digital. La capacidad de procesar información a gran escala puede ampliar significativamente el conocimiento estatal sobre las personas. Por ello, la existencia de datos técnicamente accesibles no determina por sí sola la legitimidad de su utilización en sistemas automatizados, perfiles o decisiones administrativas posteriores.

En el ordenamiento ecuatoriano, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 1, establece como objeto garantizar el ejercicio del derecho a la protección de datos personales, incluyendo el acceso y decisión sobre información de este carácter. La norma desarrolla así el mandato constitucional y proporciona reglas específicas para el tratamiento realizado mediante medios automatizados. Christodoulou y Limniotis (2024) señalan que los sistemas de decisión basados en aprendizaje automático plantean desafíos particulares para la protección de datos, debido a la complejidad del tratamiento y a las relaciones entre información de entrada, inferencias y resultados. La automatización exige, por tanto, garantías reforzadas.

La protección de datos como derecho fundamental implica que el tratamiento no puede justificarse exclusivamente por su utilidad administrativa. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece principios como juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad, confidencialidad y calidad. Estos principios limitan tanto la información que puede recopilarse como los usos posteriores que pueden realizarse mediante sistemas automatizados. Yoon et al. (2025) analizan la relación entre marcos de protección de privacidad e innovación en inteligencia artificial, evidenciando que ambas dimensiones deben examinarse conjuntamente. La innovación tecnológica no elimina la necesidad de establecer límites al tratamiento.

La autodeterminación informativa adquiere particular importancia cuando un sistema automatizado genera nuevas inferencias a partir de datos inicialmente proporcionados para otra finalidad. Una administración puede disponer de información legítimamente recopilada y, sin embargo, utilizarla posteriormente para construir perfiles, clasificaciones o predicciones que modifican sustancialmente el alcance original del tratamiento. Voloch y Hirschprung (2026) examinan la doble relación entre inteligencia artificial y privacidad, al considerar tanto los riesgos de vulneración como las posibilidades tecnológicas de protección. Este enfoque muestra que la privacidad no depende únicamente de impedir la recopilación, sino también de controlar cómo se combinan, transforman y reutilizan los datos personales durante procesos automatizados.

El derecho a la privacidad requiere igualmente garantías frente a tratamientos realizados durante todo el ciclo de vida de los sistemas de inteligencia artificial. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) establece que la privacidad debe respetarse, protegerse y promoverse durante dicho ciclo y que deben existir marcos adecuados de protección de datos. De manera complementaria, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 11, exige medidas destinadas a proteger la privacidad y los datos personales en actividades relacionadas con sistemas de inteligencia artificial.

La protección de datos adquiere una dimensión procesal cuando una persona necesita conocer qué información posee una institución y corregirla cuando resulte inexacta. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce la acción de hábeas data para acceder a documentos, datos personales e información sobre una persona, así como conocer su uso, finalidad, origen y destino en los términos constitucionalmente previstos. Esta garantía resulta especialmente relevante en sistemas automatizados, porque un dato incorrecto puede reproducirse en múltiples procedimientos. La posibilidad de acceder, rectificar o cuestionar información constituye una condición para evitar que errores administrativos se transformen en decisiones algorítmicas reiteradas.

La protección de datos también debe relacionarse con la responsabilidad institucional. Medrano-Sánchez et al. (2026) analizan la tensión entre innovación tecnológica y protección de datos en contextos de inteligencia artificial, mientras que Freitas (2026) vincula regulación, derechos civiles y gobernanza tecnológica. En el sector público, estas cuestiones adquieren especial intensidad porque el ciudadano muchas veces no puede elegir libremente si entrega determinada información cuando necesita acceder a un servicio o cumplir una obligación administrativa. Por ello, el tratamiento estatal requiere bases jurídicas claras, límites de finalidad, mecanismos de seguridad y posibilidades reales de control, especialmente cuando los datos alimentan sistemas capaces de producir consecuencias jurídicas.

En conjunto, privacidad y protección de datos funcionan como límites estructurales frente a la automatización pública. El artículo 66, numeral 19, de la Constitución de la República del Ecuador (2008), el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966), el artículo 11 de la Convención Americana sobre Derechos Humanos (1969) y el artículo 11 del Convenio Marco del Consejo de Europa (2024) muestran una convergencia en torno a la protección de la esfera personal frente a tratamientos injustificados. La administración digital

debe garantizar que el aprovechamiento de datos permanezca subordinado a derechos, finalidades legítimas, controles institucionales y mecanismos efectivos de protección.

3.2 Tratamiento de datos personales por sistemas automatizados públicos

El tratamiento de datos personales por sistemas automatizados públicos comprende operaciones mediante las cuales una institución estatal recopila, registra, organiza, consulta, combina, analiza o utiliza información relacionada con personas identificadas o identificables a través de herramientas tecnológicas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 1, establece que la protección comprende el acceso y la decisión sobre información personal, además de su correspondiente tutela. En este marco, la automatización no altera la naturaleza jurídica del tratamiento. Si una entidad pública utiliza algoritmos para procesar información ciudadana, continúa obligada a respetar los derechos del titular y las condiciones previstas por el ordenamiento.

La legitimidad del tratamiento automatizado depende de que exista una base jurídica suficiente y una finalidad determinada. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad y calidad. Estos principios obligan a justificar qué datos necesita la institución, para qué serán utilizados y durante cuánto tiempo resultan necesarios. Christodoulou y Limniotis (2024) advierten que los sistemas de decisión automatizada basados en aprendizaje automático presentan dificultades adicionales para aplicar los principios tradicionales de protección de datos, debido a la complejidad del procesamiento y a la generación de inferencias.

La transparencia constituye una obligación esencial cuando la administración emplea sistemas automatizados. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, el titular debe recibir información sobre las finalidades del tratamiento, la base legal, los tipos de tratamiento y la existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. Esta obligación permite que la persona conozca que sus datos no se utilizan únicamente para conservar un registro, sino que pueden intervenir en procesos de clasificación o evaluación. Arnesen (2026) destaca la relevancia jurídica de diferenciar el derecho a recibir información sobre decisiones automatizadas del derecho específico a obtener explicaciones.

El tratamiento automatizado adquiere mayor intensidad jurídica cuando participa directamente en decisiones que producen efectos sobre las personas. La Ley Orgánica de Protección de Datos

Personales (2021), en su artículo 20, reconoce el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La norma permite solicitar una explicación motivada, presentar observaciones, conocer criterios de valoración, identificar los tipos y fuentes de datos utilizados e impugnar la decisión. Binns y Veale (2021) muestran que determinar cuándo existe una decisión automatizada jurídicamente relevante puede resultar complejo cuando intervienen varias fases sucesivas de perfilamiento.

Las garantías sobre decisiones automatizadas adquieren una dimensión particular cuando el sistema utiliza datos para construir inferencias sobre comportamiento, riesgo o elegibilidad. Papadimitriou (2023) señala que el derecho a explicación constituye una herramienta importante para permitir que los titulares comprendan cómo el procesamiento automatizado puede afectar su posición jurídica. En el ámbito público, esta exigencia se conecta con el artículo 76 de la Constitución de la República del Ecuador (2008), que garantiza el debido proceso cuando se determinan derechos y obligaciones. Una institución no puede considerar suficiente la existencia de un resultado tecnológico si la persona afectada carece de medios para conocer y controvertir sus fundamentos relevantes.

El tratamiento automatizado por entidades públicas también debe someterse al principio de proporcionalidad. No toda finalidad administrativa justifica recopilar y procesar grandes cantidades de información personal. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que el tratamiento sea adecuado, necesario, oportuno, relevante y no excesivo respecto de las finalidades para las cuales fue obtenido. Alzoubi y Mishra (2025) analizan mecanismos técnicos de privacidad diferencial como alternativas para reducir exposición de información durante procesos analíticos. Aunque estas soluciones no sustituyen las obligaciones legales, muestran que la protección de datos puede integrarse técnicamente en el funcionamiento de sistemas que requieren análisis agregado de información ciudadana.

La seguridad constituye otra obligación inseparable del tratamiento automatizado. Los sistemas públicos pueden concentrar grandes volúmenes de información y aumentar las consecuencias de accesos indebidos, filtraciones o usos no autorizados. Voloch y Hirschprung (2026) muestran que la inteligencia artificial puede producir simultáneamente riesgos para la privacidad y herramientas orientadas a su protección. Esta doble condición obliga a las instituciones a adoptar controles técnicos y organizativos adecuados. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce expresamente la

protección de datos personales y exige autorización del titular o mandato legal para su recopilación, procesamiento, distribución o difusión según corresponda.

La automatización pública puede requerir además la interconexión de registros pertenecientes a distintas instituciones. Esta posibilidad debe evaluarse dentro de las reglas que protegen la información personal y la seguridad jurídica. La Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 1, establece que su objeto comprende la regulación, organización, sistematización e interconexión de información registral bajo criterios de eficacia, eficiencia, seguridad y transparencia. La interoperabilidad administrativa puede mejorar servicios, pero también ampliar el número de contextos en los que un dato es utilizado. Por ello, la conexión tecnológica entre bases públicas no convierte automáticamente en legítima cualquier reutilización posterior.

El derecho comparado ha desarrollado obligaciones específicas para determinados sistemas capaces de afectar derechos fundamentales. El Reglamento (UE) 2024/1689 establece en su artículo 10 requisitos de gobernanza de datos para sistemas de inteligencia artificial de alto riesgo y, en su artículo 27, contempla evaluaciones de impacto sobre derechos fundamentales para determinados responsables que utilizan esos sistemas. Estas disposiciones no constituyen derecho ecuatoriano, pero muestran una tendencia regulatoria hacia la evaluación anticipada de consecuencias. Thomaidou y Limniotis (2025) explican que las evaluaciones de impacto en protección de datos y derechos fundamentales pueden complementarse cuando el funcionamiento de la inteligencia artificial involucra información personal y decisiones relevantes.

La protección internacional refuerza los límites al tratamiento automatizado estatal. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, protege contra injerencias arbitrarias o ilegales en la vida privada. La Convención Americana sobre Derechos Humanos (1969), en su artículo 11, reconoce igualmente protección frente a injerencias arbitrarias o abusivas. Por su parte, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 11, exige medidas destinadas a garantizar privacidad y protección de datos personales durante el ciclo de vida de sistemas de inteligencia artificial. Estos estándares limitan la utilización indiscriminada de información personal.

Figura 5

Marco jurídico del tratamiento automatizado de datos personales por entidades públicas



Nota. El esquema resume los principales elementos jurídicos del tratamiento automatizado de datos personales, incluyendo sus principios, derechos del titular, obligaciones institucionales y fundamentos normativos aplicables.

El tratamiento de datos personales mediante sistemas públicos automatizados exige, finalmente, responsabilidad institucional durante todo el proceso. Medrano-Sánchez et al. (2026) muestran que la integración de inteligencia artificial y protección de datos plantea tensiones entre innovación, regulación y control de riesgos. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) exige proteger privacidad y datos durante todo el ciclo de vida de estos sistemas. En consecuencia, la administración debe conocer qué información utiliza, justificar su finalidad, garantizar derechos del titular, controlar su seguridad y revisar los efectos derivados del procesamiento. La automatización no disminuye estas obligaciones; aumenta la necesidad de hacerlas verificables.

3.3 Recolección, integración y reutilización de datos en la administración pública

La recolección de datos constituye la primera fase de numerosos procesos administrativos digitalizados y determina qué información estará disponible para posteriores análisis, cruces o decisiones automatizadas. En el sector público, esta actividad debe responder a una finalidad legítima vinculada con las competencias de la institución. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece que las finalidades del tratamiento deben ser determinadas, explícitas y legítimas, y exige que los datos sean pertinentes y limitados a lo estrictamente necesario. En consecuencia, la administración no puede recopilar información

simplemente porque exista capacidad tecnológica para almacenarla o procesarla posteriormente.

La integración de información permite combinar datos provenientes de distintas bases institucionales para obtener una visión más amplia sobre una persona, trámite o situación administrativa. La Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 1, contempla expresamente la organización, sistematización e interconexión de información como parte de sus finalidades. Sin embargo, esa interconexión no elimina las obligaciones sobre integridad, protección y control. El artículo 4 de la misma ley atribuye responsabilidad a las instituciones que administran registros y bases de datos. Por ello, integrar información exige determinar quién responde por su calidad, actualización, acceso y utilización posterior.

La reutilización plantea mayores dificultades porque un dato obtenido legítimamente para una finalidad puede resultar improcedente cuando se utiliza posteriormente con otro propósito. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, dispone que no deben tratarse datos con fines distintos de aquellos para los cuales fueron recopilados, salvo que exista una causa que habilite un nuevo tratamiento. La norma exige valorar contexto, expectativas razonables del titular, naturaleza de la información, consecuencias del nuevo uso y garantías disponibles. Esta regla resulta esencial frente a sistemas automatizados capaces de reutilizar datos administrativos para producir perfiles, predicciones o clasificaciones no previstas inicialmente.

La transferencia o comunicación entre instituciones tampoco puede entenderse como una circulación automática de información. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 33, establece condiciones para transferir o comunicar datos personales a terceros y exige que exista relación con funciones legítimas del responsable y del destinatario, además de una causal de legitimidad aplicable. La propia ley entiende por transferencia o comunicación formas como consulta, interconexión, cesión, transmisión o divulgación. En consecuencia, cuando una entidad pública consulta bases administradas por otra institución para alimentar un sistema automatizado, debe justificar jurídicamente tanto el acceso como la finalidad concreta del intercambio.

La calidad de la información constituye otra exigencia central durante integración y reutilización. La Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 3, dispone que los datos públicos registrales deben ser completos, accesibles, veraces,

verificables y pertinentes respecto de su ámbito y finalidad. A su vez, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige exactitud, integridad, precisión, completitud y actualización. Estas reglas adquieren especial relevancia en decisiones automatizadas porque una inconsistencia entre registros puede producir inferencias incorrectas. El error deja de ser meramente documental cuando se convierte en una variable utilizada por un algoritmo.

La interconexión masiva de registros puede aumentar además los riesgos de pérdida de confidencialidad. La Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 6, considera confidenciales determinados datos personales y dispone que su acceso solo procede con autorización expresa del titular, mandato legal u orden judicial, según corresponda. El mismo artículo exige a las autoridades custodias adoptar medidas necesarias para proteger la reserva de la información. Esta obligación demuestra que la existencia de infraestructura interoperable no equivale a disponibilidad irrestricta. La administración debe diferenciar datos públicos, datos personales y datos sujetos a confidencialidad antes de integrarlos en plataformas automatizadas.

La reutilización también puede generar información nueva que no existía explícitamente en las bases originales. Al combinar antecedentes laborales, territoriales, económicos, sanitarios o administrativos, un sistema puede inferir niveles de riesgo, vulnerabilidad o probabilidad de incumplimiento. Voloch y Hirschprung (2026) advierten que la inteligencia artificial puede ampliar significativamente los riesgos para la privacidad precisamente por su capacidad de extraer relaciones y patrones de grandes volúmenes de datos. En el ámbito público, estas inferencias requieren especial control porque pueden terminar condicionando decisiones posteriores. La legitimidad de poseer cada dato individual no significa necesariamente que toda inferencia derivada de su combinación sea jurídicamente admisible.

La protección constitucional establece un límite adicional a estas prácticas. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce el derecho a la protección de datos personales y exige autorización del titular o mandato legal para su recolección, archivo, procesamiento, distribución o difusión, según corresponda. Asimismo, el artículo 92 permite conocer la existencia, uso, finalidad, origen y destino de información personal mediante hábeas data. Estas garantías resultan especialmente importantes cuando la información se mueve entre varias entidades, porque la persona puede desconocer qué institución conserva actualmente sus datos o para qué finalidad fueron reutilizados dentro de un procedimiento automatizado.

Desde la perspectiva internacional, el derecho a la privacidad limita también la integración indiscriminada de registros administrativos. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe injerencias arbitrarias o ilegales en la vida privada, mientras que la Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege frente a injerencias arbitrarias o abusivas. Estos estándares obligan a examinar necesidad y proporcionalidad del tratamiento estatal. La posibilidad técnica de cruzar bases de datos no constituye por sí sola una justificación suficiente. La administración debe demostrar que la integración responde a una finalidad legítima y que no existen medios menos invasivos.

La regulación comparada refuerza la necesidad de una gobernanza estructurada de los datos. El Reglamento (UE) 2024/1689, en su artículo 10, exige para determinados sistemas de alto riesgo prácticas de gobernanza relacionadas con recopilación, preparación, representatividad, pertinencia y calidad de los conjuntos utilizados. Alzoubi y Mishra (2025) muestran además que técnicas de privacidad diferencial pueden reducir la exposición de información individual durante determinados procesos analíticos. Estas soluciones no sustituyen las obligaciones jurídicas, pero evidencian que la protección puede incorporarse desde el diseño tecnológico. La administración debe combinar medidas normativas, organizativas y técnicas cuando integra grandes volúmenes de información personal.

La recolección, integración y reutilización de datos públicos debe entenderse, finalmente, como una cadena de responsabilidad y no como etapas aisladas. Cada operación modifica las posibilidades futuras de utilización de la información y puede aumentar tanto su valor administrativo como el riesgo para los derechos. La Ley Orgánica de Protección de Datos Personales (2021), especialmente en sus artículos 10 y 33, y la Ley del Sistema Nacional de Registro de Datos Públicos (2010), en sus artículos 3, 4 y 6, establecen límites relacionados con finalidad, calidad, responsabilidad, transferencia y confidencialidad. La automatización exige que estos controles acompañen cada movimiento de los datos dentro del Estado.

3.4 Perfilamiento ciudadano y elaboración automatizada de perfiles

El perfilamiento ciudadano consiste en utilizar datos personales para evaluar o predecir aspectos relacionados con una persona, como comportamiento, situación económica, preferencias, nivel de riesgo o probabilidad de cumplir determinadas condiciones. En la administración pública, estas prácticas pueden emplearse para clasificar expedientes, priorizar controles, asignar prestaciones o identificar posibles irregularidades. Binns y Veale (2021) muestran que el perfilamiento puede intervenir en varias etapas de una decisión y dificultar la

identificación del momento exacto en que el resultado adquiere efectos jurídicos. Esta complejidad exige analizar no solo la decisión final, sino también las clasificaciones automatizadas que contribuyeron materialmente a producirla.

La elaboración automatizada de perfiles depende de la combinación de datos y de inferencias generadas mediante reglas o modelos algorítmicos. Un sistema puede partir de información aparentemente fragmentada y convertirla en categorías como riesgo alto, prioridad, vulnerabilidad o probabilidad de incumplimiento. Voloch y Hirschprung (2026) advierten que la inteligencia artificial amplía los riesgos para la privacidad al permitir extraer relaciones y características que no estaban expresamente contenidas en cada dato individual. En el ámbito público, estas inferencias adquieren relevancia jurídica porque pueden utilizarse posteriormente como fundamento de actuaciones administrativas que afecten derechos, oportunidades o acceso a servicios estatales.

El ordenamiento ecuatoriano establece garantías expresas frente a este tipo de tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La persona puede solicitar una explicación motivada, formular observaciones, conocer los criterios de valoración, obtener información sobre los tipos y fuentes de datos utilizados e impugnar la decisión. Estas garantías muestran que el perfilamiento deja de ser una operación meramente técnica cuando condiciona materialmente una decisión administrativa.

La transparencia resulta fundamental porque una persona puede desconocer que está siendo clasificada mediante un perfil automatizado. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, obliga a informar sobre la existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles, cuando corresponda. Arnesen (2026) distingue entre recibir información acerca de la existencia del procesamiento automatizado y obtener una explicación suficientemente útil sobre su funcionamiento y consecuencias. Esta diferencia resulta relevante en la administración pública: informar simplemente que se utilizó un algoritmo no permite comprender qué datos fueron determinantes, cómo se construyó la clasificación o qué posibilidades existen de cuestionarla.

El perfilamiento puede generar además riesgos de discriminación cuando las categorías creadas se correlacionan con condiciones protegidas o situaciones de vulnerabilidad. Freitas (2026)

vincula la regulación de inteligencia artificial con protección de datos y derechos civiles, mientras que Thomaïdou y Limniotis (2025) destacan la utilidad de las evaluaciones de impacto para identificar efectos sobre derechos fundamentales. En Ecuador, el artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) prohíbe distinciones cuyo objeto o resultado menoscabe derechos. Por ello, una clasificación automatizada aparentemente neutral debe revisarse cuando produce efectos sistemáticamente desfavorables para determinados grupos de población.

Tabla 8

Elementos jurídicos del perfilamiento ciudadano automatizado

Elemento	Función en el perfilamiento	Riesgo principal	Garantía aplicable
Datos de entrada	Alimentan el sistema con información personal	Información incorrecta, excesiva o desactualizada	Calidad, finalidad y minimización de datos
Variables de clasificación	Determinan qué características serán consideradas	Uso de variables proxy o discriminatorias	Igualdad y no discriminación
Modelo algorítmico	Identifica patrones y asigna categorías	Opacidad o errores sistemáticos	Transparencia y supervisión
Perfil resultante	Resume características, riesgo o probabilidad	Estigmatización o clasificación permanente	Derecho a conocer y cuestionar el perfil
Decisión posterior	Utiliza el perfil para una actuación administrativa	Efectos jurídicos desfavorables	Explicación e impugnación
Reutilización	Emplea el perfil en procedimientos posteriores	Ampliación de una clasificación fuera de su finalidad inicial	Limitación de finalidad
Actualización	Modifica el perfil con nuevos datos	Permanencia de inferencias incorrectas	Rectificación y revisión periódica

Nota. El perfil automatizado debe analizarse como un proceso completo que comprende datos, inferencias, clasificación y utilización posterior del resultado, especialmente cuando puede afectar derechos.

El derecho de acceso adquiere especial relevancia frente a perfiles que la persona no puede observar directamente. Custers y Heijne (2022) analizan el alcance del acceso a información relacionada con decisiones automatizadas y muestran que la posibilidad de conocer datos y lógica relevante constituye una condición para ejercer otros derechos. En Ecuador, la Constitución de la República del Ecuador (2008), en su artículo 92, reconoce la acción de hábeas data para conocer la existencia, uso, finalidad, origen y destino de información personal. Esta garantía puede ser especialmente útil cuando un perfil automatizado contiene datos incorrectos o inferencias que afectan sucesivamente diferentes procedimientos públicos.

La elaboración de perfiles también debe respetar el derecho a la privacidad reconocido internacionalmente. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe injerencias arbitrarias o ilegales en la vida privada, mientras que la Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege frente a injerencias arbitrarias o abusivas. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 11, exige medidas para proteger privacidad y datos personales durante el ciclo de vida de los sistemas de inteligencia artificial.

Desde el derecho comparado, el Reglamento (UE) 2024/1689 refuerza la evaluación previa cuando determinados sistemas de alto riesgo son utilizados por organismos públicos. Su artículo 27 exige una evaluación de impacto sobre derechos fundamentales que identifique las categorías de personas potencialmente afectadas, los riesgos de daño y las medidas de supervisión y mitigación. Esta exigencia resulta especialmente pertinente para sistemas de perfilamiento utilizados en prestaciones, control o servicios públicos. Aunque la norma no es directamente aplicable en Ecuador, proporciona un criterio relevante: antes de utilizar perfiles automatizados, la institución debería analizar qué grupos serán clasificados, qué consecuencias pueden derivarse y cómo podrán cuestionarse los resultados.

El perfilamiento ciudadano exige, finalmente, evitar que las inferencias tecnológicas se conviertan en atributos permanentes de las personas. Una clasificación puede haber sido válida en un contexto determinado y resultar incorrecta posteriormente, especialmente cuando cambian circunstancias personales o los datos de origen. Medrano-Sánchez et al. (2026) destacan la tensión entre innovación basada en inteligencia artificial y protección efectiva de datos personales. La administración debe establecer mecanismos de actualización, revisión y eliminación cuando corresponda. El artículo 20 de la Ley Orgánica de Protección de Datos Personales (2021) refuerza esta exigencia al permitir cuestionar valoraciones automatizadas con efectos jurídicos, incluida expresamente la elaboración de perfiles.

3.5 Datos sensibles y riesgos derivados de su procesamiento automatizado

Los datos sensibles requieren una protección reforzada porque revelan aspectos de la persona cuya utilización indebida puede producir discriminación, exclusión, estigmatización o afectaciones graves a la privacidad. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 25, identifica categorías especiales de datos, entre ellas aquellos relacionados con salud, origen étnico, identidad de género, orientación sexual, convicciones religiosas o

filosóficas y otros datos capaces de generar riesgos particulares. Cuando estas categorías son procesadas mediante sistemas automatizados, el problema aumenta porque una clasificación puede reproducirse a gran escala y afectar decisiones posteriores sobre acceso a servicios, controles o prestaciones públicas.

El procesamiento automatizado de datos sensibles puede generar inferencias que trascienden la información originalmente recopilada. Un sistema puede combinar antecedentes sanitarios, laborales, territoriales o administrativos y producir perfiles sobre vulnerabilidad, riesgo o comportamiento futuro. Murdoch (2021) advierte que la inteligencia artificial aplicada a información de salud plantea desafíos relevantes para la privacidad debido al volumen y detalle de los datos procesados. En el sector público, estas inferencias deben evaluarse con especial cautela porque pueden condicionar decisiones institucionales sin que la persona conozca cómo fueron construidas. La existencia de datos sensibles legítimamente obtenidos no autoriza cualquier reutilización automatizada posterior.

La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce el derecho a la protección de datos personales y exige autorización del titular o mandato legal para su recopilación, procesamiento, distribución o difusión, según corresponda. A ello se suma el artículo 66, numeral 20, que reconoce el derecho a la intimidad personal y familiar. Estas garantías establecen límites frente al tratamiento automatizado de información especialmente delicada. Cuando una entidad pública utiliza datos sensibles, debe demostrar que la finalidad es legítima, que el tratamiento resulta necesario y que existen salvaguardas suficientes para evitar usos incompatibles con los derechos de las personas afectadas.

La utilización de datos sensibles puede producir discriminación cuando la información se incorpora como variable directa o indirecta en modelos de clasificación. Wang et al. (2024) muestran que la discriminación algorítmica puede surgir mediante variables proxy, selección de características y efectos diferenciados. Esta situación es especialmente problemática cuando un sistema utiliza datos de salud, condición socioeconómica, procedencia o características personales para asignar categorías de riesgo. La prohibición de discriminación contenida en el artículo 11, numeral 2, de la Constitución de la República del Ecuador (2008) obliga a revisar tanto el uso explícito de estas variables como los resultados indirectos derivados de su combinación algorítmica.

Los riesgos también se relacionan con la seguridad de la información. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023) desarrolla obligaciones vinculadas

con medidas técnicas y organizativas destinadas a garantizar confidencialidad, integridad y seguridad del tratamiento. En sistemas automatizados, una vulneración puede afectar simultáneamente grandes volúmenes de datos sensibles y facilitar usos posteriores no autorizados. Voloch y Hirschprung (2026) señalan que la inteligencia artificial puede intensificar riesgos de privacidad, aunque también puede utilizarse para desarrollar mecanismos de protección. La administración debe adoptar medidas de seguridad desde el diseño y mantener controles durante toda la vida útil del sistema.

Tabla 9

Riesgos asociados con el procesamiento automatizado de datos sensibles

Tipo de dato sensible	Posible uso automatizado	Riesgo principal	Garantía jurídica relevante
Datos de salud	Clasificación de riesgo o priorización de servicios	Estigmatización o exclusión	Constitución, art. 66, núms. 19 y 20; LOPDP, art. 25
Origen étnico	Segmentación o análisis poblacional	Discriminación directa o indirecta	Constitución, art. 11, núm. 2
Identidad de género u orientación sexual	Perfilamiento o segmentación	Trato diferenciado injustificado	Constitución, art. 11, núm. 2
Convicciones religiosas o filosóficas	Construcción de perfiles	Injerencia en la vida privada	PIDCP, art. 17; CADH, art. 11
Datos biométricos	Identificación o autenticación automatizada	Vigilancia, suplantación o exclusión	LOPDP, art. 25
Información socioeconómica	Evaluación de elegibilidad o riesgo	Discriminación por condición económica	Constitución, art. 11, núm. 2
Datos combinados	Inferencias automatizadas	Creación de perfiles no previstos	LOPDP, arts. 10 y 20

Nota. El riesgo aumenta cuando varias categorías sensibles se combinan y generan inferencias utilizadas posteriormente en decisiones administrativas.

La especial protección de estos datos se vincula también con el principio de minimización. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que los datos sean pertinentes y limitados a lo estrictamente necesario respecto de la finalidad del tratamiento. En consecuencia, una institución pública no debería incorporar información sensible a un sistema automatizado si puede alcanzar el mismo objetivo mediante datos menos invasivos. Alzoubi y Mishra (2025) examinan técnicas de privacidad diferencial como mecanismos capaces de reducir exposición individual durante determinados procesos

analíticos. Estas soluciones técnicas pueden complementar, pero no sustituir, la obligación jurídica de limitar previamente la cantidad de información utilizada.

La protección internacional refuerza estos límites. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe injerencias arbitrarias o ilegales en la vida privada, mientras que la Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege frente a injerencias arbitrarias o abusivas. La Declaración Universal de Derechos Humanos (1948), en su artículo 12, contiene una garantía equivalente. Cuando un sistema automatizado procesa datos sensibles, estas disposiciones exigen valorar necesidad, proporcionalidad y finalidad, especialmente cuando la información puede revelar aspectos íntimos que no resultan indispensables para la decisión administrativa correspondiente.

La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) insiste en que la privacidad y la protección de datos deben mantenerse durante todo el ciclo de vida de los sistemas de inteligencia artificial. Asimismo, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 11, exige medidas destinadas a proteger privacidad y datos personales. Estos estándares muestran que la protección no debe aparecer únicamente después de una filtración o daño. La administración debe evaluar previamente qué categorías sensibles procesará, qué inferencias podrían derivarse y qué medidas evitarán usos incompatibles con los derechos fundamentales.

Desde el derecho comparado, el Reglamento (UE) 2024/1689 refuerza la necesidad de controles específicos cuando sistemas de alto riesgo utilizan datos relevantes para decisiones que afectan derechos. Su artículo 10 exige prácticas de gobernanza relacionadas con calidad, pertinencia y representatividad de los conjuntos de datos. Estas obligaciones resultan especialmente relevantes cuando la información pertenece a categorías sensibles o puede producir efectos discriminatorios. Aunque la norma no es directamente aplicable en Ecuador, ofrece un criterio útil: cuanto mayor sea la sensibilidad de la información y la gravedad de la decisión, mayor debe ser la intensidad de los controles técnicos, jurídicos y organizativos.

El procesamiento automatizado de datos sensibles exige, finalmente, una evaluación reforzada de riesgos. Thomaidou y Limniotis (2025) muestran que las evaluaciones de impacto pueden articular protección de datos y derechos fundamentales cuando sistemas de inteligencia artificial operan sobre información personal. En el ámbito público, esta evaluación debe considerar posibles discriminaciones, errores, accesos indebidos, usos secundarios e

inferencias no previstas. La administración debe justificar por qué necesita utilizar datos sensibles, qué medidas de seguridad aplicará y cómo podrá la persona ejercer sus derechos. La utilización de estas categorías solo resulta legítima cuando existe una base jurídica clara y salvaguardas proporcionales al nivel de riesgo.

3.6 Principios de protección de datos aplicables a la automatización pública

Los principios de protección de datos constituyen criterios jurídicos obligatorios para cualquier tratamiento automatizado realizado por instituciones públicas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece principios de juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad, confidencialidad, calidad y conservación, entre otros. Su aplicación resulta especialmente relevante cuando algoritmos procesan grandes volúmenes de información o generan inferencias utilizadas posteriormente en decisiones administrativas. Christodoulou y Limniotis (2024) advierten que el aprendizaje automático plantea dificultades específicas para aplicar estos principios, debido a la complejidad de los modelos y al carácter dinámico del tratamiento de información personal.

El principio de juridicidad exige que todo tratamiento de datos personales encuentre fundamento en una base jurídica válida. En el ámbito público, esta exigencia se relaciona además con el artículo 226 de la Constitución de la República del Ecuador (2008), según el cual las instituciones estatales solo pueden ejercer las competencias y facultades atribuidas por la Constitución y la ley. Asimismo, el artículo 14 del Código Orgánico Administrativo (2017) somete la actuación administrativa al principio de juridicidad. Por tanto, una entidad no puede procesar datos mediante sistemas automatizados únicamente porque la tecnología permita hacerlo; debe existir competencia, finalidad legítima y habilitación jurídica suficiente para efectuar ese tratamiento.

El principio de finalidad exige que los datos sean recopilados y tratados para objetivos determinados, explícitos y legítimos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, impide que la información sea reutilizada indiscriminadamente para finalidades incompatibles con aquellas que justificaron su obtención. Esta exigencia adquiere especial importancia en sistemas automatizados capaces de combinar bases administrativas y generar nuevos perfiles o inferencias. Yoon et al. (2025) muestran que los marcos de protección de privacidad condicionan la relación entre innovación y utilización de inteligencia artificial. En consecuencia, la disponibilidad técnica de información no elimina la obligación de respetar la finalidad inicialmente definida.

El principio de minimización obliga a utilizar únicamente los datos estrictamente necesarios para alcanzar la finalidad legítima del tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige pertinencia y proporcionalidad de la información procesada. En sistemas automatizados, este principio resulta particularmente relevante porque aumentar el número de variables puede incrementar simultáneamente la capacidad predictiva y los riesgos de privacidad, discriminación o perfilamiento. Alzoubi y Mishra (2025) analizan técnicas de privacidad diferencial orientadas a reducir exposición individual en contextos de inteligencia artificial. Estas soluciones pueden complementar la minimización, pero no reemplazan la obligación previa de justificar cada categoría de datos utilizada.

El principio de transparencia exige que las personas conozcan de manera comprensible cómo se tratan sus datos y con qué finalidades. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho a recibir información sobre el tratamiento y sobre la existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. Custers y Heijne (2022) destacan que el acceso a información relacionada con decisiones automatizadas resulta esencial para ejercer derechos posteriores. En la administración pública, esta transparencia debe permitir identificar qué información se utilizó, de dónde provino y qué papel tuvo dentro de la actuación administrativa correspondiente.

La calidad constituye otro principio central porque las decisiones automatizadas dependen directamente de la exactitud y actualización de los datos procesados. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige exactitud, integridad, precisión, completitud y actualización. Asimismo, la Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 3, establece que los datos públicos registrales deben ser completos, accesibles, veraces, verificables y pertinentes. La utilización de información incorrecta puede generar clasificaciones erróneas que se reproduzcan automáticamente. Por ello, la administración debe establecer procedimientos de validación y rectificación antes de utilizar registros públicos como insumos algorítmicos.

El principio de confidencialidad exige prevenir accesos, comunicaciones o utilidades no autorizadas. La Ley del Sistema Nacional de Registro de Datos Públicos (2010), en su artículo 6, reconoce el carácter confidencial de determinados datos personales y obliga a las autoridades responsables a proteger su reserva. A su vez, el Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023) desarrolla medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento. Voloch y Hirschprung (2026) advierten que la inteligencia artificial puede intensificar amenazas para la privacidad debido a su capacidad para

combinar y analizar información, aunque también permite incorporar herramientas técnicas de protección.

La conservación de datos debe estar limitada al tiempo necesario para cumplir la finalidad que justificó su tratamiento. En contextos automatizados, la acumulación indefinida de información puede generar perfiles cada vez más detallados y ampliar usos que no estaban previstos inicialmente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora la conservación como principio vinculado con la duración necesaria del tratamiento. Medrano-Sánchez et al. (2026) señalan que la expansión de inteligencia artificial plantea tensiones entre innovación y protección efectiva de información personal. La administración debe definir plazos, criterios de archivo y mecanismos de eliminación o anonimización cuando desaparezca la finalidad legítima.

Figura 6

Principios de protección de datos - LOPDP Art. 10



Nota. Adaptado de LOPDP (2021), Constitución (2008) y Ley de Registro de Datos Públicos (2010). El centro representa el tratamiento automatizado por algoritmos en la administración pública.

El principio de responsabilidad exige que la institución pueda demostrar que cumple las obligaciones asociadas con el tratamiento automatizado. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) sostiene que la responsabilidad y rendición de cuentas deben mantenerse durante todo el ciclo de vida de los sistemas de inteligencia artificial. De manera complementaria, el Convenio Marco del Consejo de Europa sobre Inteligencia

Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 11, exige medidas destinadas a proteger privacidad y datos personales. La administración debe documentar decisiones de diseño, fuentes de datos, evaluaciones de riesgo, mecanismos de seguridad y procedimientos utilizados para atender derechos.

Los principios de protección de datos también deben integrarse con un enfoque preventivo basado en riesgos. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 10 obligaciones de gobernanza de datos para sistemas de inteligencia artificial de alto riesgo, incluyendo aspectos de pertinencia, representatividad y calidad. Thomaidou y Limniotis (2025) muestran que las evaluaciones de impacto sobre protección de datos y derechos fundamentales pueden complementarse para identificar riesgos antes de implementar sistemas automatizados. Este enfoque permite anticipar problemas relacionados con privacidad, discriminación, seguridad o errores y establecer medidas correctivas antes de que los resultados tecnológicos produzcan consecuencias administrativas difíciles de revertir.

En conjunto, los principios de juridicidad, finalidad, minimización, transparencia, calidad, confidencialidad, conservación y responsabilidad delimitan jurídicamente la automatización pública basada en datos personales. Su aplicación permite evaluar no solo si una institución puede procesar información, sino también cómo debe hacerlo y bajo qué condiciones. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce el derecho a la protección de datos personales, mientras que la Ley Orgánica de Protección de Datos Personales (2021), especialmente en su artículo 10, desarrolla los principios que concretan este derecho. La automatización resulta admisible cuando estos principios permanecen verificables durante todo el tratamiento.

3.7 Límites jurídicos al uso de datos personales en decisiones automatizadas

El uso de datos personales en decisiones automatizadas encuentra su primer límite en la necesidad de una base jurídica suficiente. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, establece que la recolección, archivo, procesamiento, distribución o difusión de datos personales requiere autorización del titular o mandato legal. Esta exigencia impide que una entidad pública utilice información ciudadana únicamente porque dispone de ella técnicamente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 2, confirma además que sus garantías se aplican al tratamiento automatizado y a toda modalidad de uso posterior de datos personales.

Un segundo límite se relaciona con la finalidad y proporcionalidad del tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que la utilización de información responda a finalidades determinadas, explícitas y legítimas y que los datos sean pertinentes y limitados a lo necesario. En sistemas automatizados, esta obligación impide incorporar indiscriminadamente variables solo porque puedan mejorar capacidad predictiva. Christodoulou y Limniotis (2024) advierten que los modelos de aprendizaje automático plantean dificultades específicas para aplicar los principios tradicionales de protección de datos. La eficiencia predictiva no basta para justificar un tratamiento que resulte excesivo respecto del objetivo administrativo perseguido.

La intervención automatizada encuentra un límite especialmente claro cuando produce efectos jurídicos sobre la persona. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a no ser sometido a decisiones basadas única o parcialmente en valoraciones automatizadas, incluida la elaboración de perfiles, cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La norma permite solicitar explicación motivada, formular observaciones, conocer criterios de valoración, identificar las fuentes de datos e impugnar la decisión. Bayamlioğlu (2022) destaca precisamente la importancia del derecho a controvertir decisiones automatizadas como garantía distinta de la mera obtención de información.

La protección resulta aún más estricta cuando intervienen niñas, niños y adolescentes. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 21, establece garantías específicas frente a decisiones basadas total o parcialmente en valoraciones automatizadas y limita el tratamiento de datos sensibles o de menores salvo autorización válida o existencia de un interés público esencial conforme a los estándares aplicables. Este límite responde a la especial vulnerabilidad de estas personas frente a perfiles o clasificaciones que podrían condicionar servicios, prestaciones o evaluaciones futuras. La automatización pública debe evitar que una inferencia temprana se convierta en una categoría permanente con consecuencias difíciles de modificar posteriormente.

La administración también está obligada a evaluar anticipadamente los tratamientos capaces de generar riesgos elevados. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 42, exige una evaluación de impacto cuando la naturaleza, contexto o finalidad del tratamiento pueda generar alto riesgo para derechos y libertades. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023), en su artículo 29, define esta evaluación como un análisis preventivo dirigido a identificar y mitigar riesgos. Thomaidou y

Limnriotis (2025) sostienen que estas evaluaciones permiten vincular protección de datos con impactos más amplios sobre derechos fundamentales derivados de sistemas de inteligencia artificial.

Tabla 10

Principales límites jurídicos al uso de datos personales en decisiones automatizadas

Límite jurídico	Riesgo que pretende evitar	Fundamento principal	Consecuencia para la administración
Base jurídica	Tratamiento arbitrario de información	Constitución, art. 66.19; LOPDP, art. 2	Justificar legalmente el procesamiento
Finalidad y minimización	Uso excesivo o incompatible de datos	LOPDP, art. 10	Utilizar únicamente información necesaria
Control de decisiones automatizadas	Afectaciones jurídicas sin revisión	LOPDP, art. 20	Explicar, permitir observaciones e impugnación
Protección reforzada de menores	Perfilamiento y efectos desproporcionados	LOPDP, art. 21	Aplicar garantías adicionales
Evaluación de impacto	Riesgos elevados para derechos	LOPDP, art. 42; Reglamento, art. 29	Evaluar y mitigar riesgos previamente
Privacidad	Injerencias arbitrarias o abusivas	PIDCP, art. 17; CADH, art. 11	Justificar necesidad y proporcionalidad
Tutela judicial	Imposibilidad de corregir datos o decisiones	Constitución, art. 92; LOGJCC, arts. 49–50	Garantizar acceso, rectificación y protección judicial

Nota. Los límites jurídicos se aplican durante todo el ciclo del tratamiento y aumentan en intensidad cuando la decisión automatizada puede producir efectos jurídicos o afectar derechos fundamentales.

El derecho a la privacidad opera como límite adicional frente a la expansión del tratamiento automatizado. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe injerencias arbitrarias o ilegales en la vida privada, mientras que la Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege frente a injerencias arbitrarias o abusivas. Estas disposiciones obligan a valorar necesidad y proporcionalidad del procesamiento estatal. Yoon et al. (2025) muestran que los marcos de protección de privacidad inciden directamente en las condiciones bajo las cuales puede desarrollarse innovación basada en inteligencia artificial. La disponibilidad de datos no equivale, por tanto, a libertad absoluta para utilizarlos.

La posibilidad de impugnar y corregir información constituye otro límite esencial. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce el hábeas data

para conocer la existencia, uso, finalidad, origen y destino de los datos personales y solicitar su actualización, rectificación, eliminación o anulación. La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en sus artículos 49 y 50, desarrolla esta garantía y permite acudir judicialmente cuando se niega el acceso o no se atienden solicitudes relacionadas con datos que puedan afectar derechos. En sistemas automatizados, esta vía adquiere importancia cuando una información errónea condiciona reiteradamente decisiones administrativas posteriores.

El derecho comparado refuerza la necesidad de límites preventivos. El Reglamento (UE) 2024/1689, en su artículo 27, exige evaluaciones de impacto sobre derechos fundamentales para determinados usos de sistemas de inteligencia artificial de alto riesgo, mientras que su artículo 14 establece supervisión humana. El Convenio Marco del Consejo de Europa (2024), en sus artículos 11 y 16, vincula protección de datos con evaluación y mitigación de riesgos durante el ciclo de vida de los sistemas de inteligencia artificial. Aunque estas normas no constituyen legislación ecuatoriana, ofrecen criterios útiles para evaluar cuándo el procesamiento automatizado requiere controles reforzados, documentación y posibilidades efectivas de revisión.

Los límites jurídicos al uso de datos personales no pretenden impedir la automatización pública, sino evitar que su desarrollo debilite derechos fundamentales. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) exige proteger privacidad, dignidad y autonomía durante todo el ciclo de vida de los sistemas de inteligencia artificial. Binns y Veale (2021) muestran además que la existencia de varias fases de perfilamiento puede dificultar determinar cuándo una decisión se vuelve jurídicamente relevante. Por ello, la administración debe controlar datos, inferencias y resultados desde su origen, garantizando base jurídica, proporcionalidad, evaluación de riesgos, revisión humana y mecanismos efectivos de tutela.

Capítulo 4

Transparencia y explicación de decisiones automatizadas

Carolina Calderón Muñoz



4.1 Transparencia administrativa en entornos de automatización

La transparencia administrativa adquiere una dimensión específica cuando las decisiones públicas incorporan sistemas automatizados, porque la ciudadanía necesita conocer no solo el contenido final de la actuación, sino también el papel que desempeñó la tecnología dentro del procedimiento. Grimmeliikhuijsen (2023) muestra que la transparencia algorítmica influye en la percepción de confiabilidad de las decisiones automatizadas. En el ámbito público, esta exigencia permite identificar si un algoritmo intervino en la clasificación, priorización o recomendación de un caso. La opacidad tecnológica puede dificultar el control de legalidad cuando impide reconstruir cómo se produjo una decisión que afecta derechos o intereses individuales.

La Constitución de la República del Ecuador (2008), en su artículo 18, reconoce el derecho de todas las personas a buscar, recibir, intercambiar, producir y difundir información veraz, verificada y contextualizada, así como a acceder libremente a la información generada en entidades públicas. Este derecho resulta directamente relevante cuando una institución utiliza sistemas automatizados para apoyar decisiones administrativas. La existencia de tecnología no elimina la obligación estatal de proporcionar información sobre su actuación. Por el contrario, cuando el procedimiento incorpora componentes técnicos complejos, la administración debe garantizar que la ciudadanía pueda conocer los elementos esenciales que expliquen cómo se produjo el resultado institucional.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) desarrolla este derecho y obliga a las instituciones sujetas a la ley a garantizar acceso a la información pública. En entornos automatizados, esto comprende la necesidad de documentar la existencia de sistemas, sus finalidades, los procedimientos en los que intervienen y los criterios generales que estructuran su utilización, siempre dentro de los límites legales de reserva o confidencialidad. Custers y Heijne (2022) destacan que el acceso a información sobre procesos automatizados permite ejercer otros derechos relacionados con revisión y oposición. Sin transparencia suficiente, la posibilidad de cuestionar una decisión se debilita sustancialmente.

La transparencia debe diferenciarse de la simple publicación de información técnica. Un sistema puede contar con documentación extensa y, aun así, resultar incomprensible para la persona afectada. Dexe et al. (2022) muestran que el derecho a recibir información significativa sobre decisiones automatizadas exige considerar qué tipo de explicación resulta realmente útil para comprender el funcionamiento y las consecuencias del sistema. En la administración

pública, esto implica traducir aspectos técnicos a términos comprensibles, identificar factores relevantes y explicar el papel de la automatización en el resultado. La transparencia efectiva exige inteligibilidad y no una acumulación de documentos que solo puedan interpretar especialistas.

La obligación de informar también aparece en la normativa ecuatoriana de protección de datos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho del titular a recibir información sobre el tratamiento, incluida la existencia de valoraciones y decisiones automatizadas y la elaboración de perfiles. Esta disposición resulta especialmente relevante cuando una decisión pública utiliza datos personales para clasificar o evaluar a una persona. La transparencia, en este contexto, debe permitir conocer qué información fue utilizada, cuál fue la finalidad del tratamiento y qué consecuencias puede producir el procesamiento automatizado sobre la situación jurídica del titular.

La transparencia también exige conservar trazabilidad suficiente sobre el funcionamiento del sistema. Si una decisión automatizada no puede reconstruirse posteriormente, se dificulta determinar qué datos fueron utilizados, qué reglas intervinieron y qué responsabilidad correspondió a cada actor. Cheong (2024) relaciona transparencia y rendición de cuentas con la necesidad de proteger a las personas frente a sistemas de inteligencia artificial. En el ámbito administrativo, la trazabilidad permite revisar errores, detectar desviaciones y responder reclamaciones. La documentación interna del sistema no debe entenderse únicamente como una exigencia técnica, sino como una condición para que la actuación pública pueda ser auditada y explicada jurídicamente.

El deber de transparencia encuentra además respaldo en el Código Orgánico Administrativo (2017), cuyo artículo 18 reconoce el principio de interdicción de la arbitrariedad y exige que las actuaciones administrativas se sustenten en criterios objetivos y racionales. Aunque la norma no se refiere específicamente a algoritmos, su aplicación resulta pertinente cuando una decisión automatizada utiliza criterios que la persona no puede conocer ni cuestionar. Una actuación pública basada en reglas ocultas o no verificables puede dificultar la evaluación de racionalidad y legalidad. La automatización no exime a la administración de justificar por qué adoptó una decisión ni de demostrar que los criterios utilizados fueron legítimos y pertinentes.

La transparencia algorítmica también se relaciona con la igualdad y la no discriminación. Si una institución desconoce cómo funciona un sistema o no analiza sus resultados, puede pasar por alto patrones diferenciados de exclusión o error. Arnesen (2026) distingue entre el derecho

a recibir información sobre decisiones automatizadas y el derecho a obtener una explicación más sustantiva. Esta diferencia resulta importante porque conocer que se utilizó un algoritmo no basta para identificar posibles sesgos. La administración debe poder explicar qué factores influyeron en el resultado y ofrecer información suficiente para que la persona evalúe si existió un trato desigual o injustificado.

Desde una perspectiva internacional, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, establece obligaciones relacionadas con transparencia y supervisión en el uso de sistemas de inteligencia artificial. De manera complementaria, la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) identifica transparencia y explicabilidad como principios necesarios para una gobernanza responsable. Estos instrumentos muestran una tendencia hacia la exigencia de que los sistemas públicos sean comprensibles, auditables y sujetos a control. La transparencia no constituye un elemento accesorio, sino una condición para preservar legitimidad institucional.

El Reglamento (UE) 2024/1689 refuerza esta orientación desde el derecho comparado. Su artículo 13 establece requisitos de transparencia para sistemas de inteligencia artificial de alto riesgo, de manera que su funcionamiento sea suficientemente comprensible para quienes los utilizan. Además, el artículo 86 reconoce, en determinados supuestos, el derecho de las personas afectadas a obtener explicaciones sobre decisiones individuales tomadas a partir de sistemas de alto riesgo. Aunque este régimen no constituye derecho aplicable directamente en Ecuador, ofrece un parámetro relevante para analizar hasta qué punto la administración debe documentar, explicar y permitir el control de sistemas automatizados con impacto significativo sobre derechos.

La transparencia administrativa en entornos automatizados exige, finalmente, combinar acceso a la información, trazabilidad, explicación comprensible y rendición de cuentas. La Constitución de la República del Ecuador (2008), en su artículo 18, y la Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) proporcionan el fundamento interno, mientras que el Consejo de Europa (2024), la UNESCO (2021) y el Reglamento (UE) 2024/1689 ofrecen estándares complementarios. La automatización pública solo puede considerarse compatible con una administración transparente cuando permite conocer la intervención del sistema, comprender sus criterios relevantes, identificar responsabilidades y cuestionar las decisiones que produzca.

4.2 Opacidad algorítmica y dificultades para comprender la decisión pública

La opacidad algorítmica aparece cuando las personas afectadas, los funcionarios responsables o incluso la propia institución encuentran dificultades para comprender cómo un sistema automatizado produjo determinado resultado. Esta opacidad puede derivar de modelos técnicamente complejos, falta de documentación, uso de proveedores externos o ausencia de información accesible sobre variables y criterios. Peters (2023) advierte que la opacidad de los sistemas de inteligencia artificial no puede equipararse sin más con la opacidad de las decisiones humanas, porque los mecanismos de justificación y control son diferentes. En la administración pública, esta dificultad compromete directamente la capacidad de revisar y cuestionar decisiones con efectos jurídicos.

La opacidad puede ser técnica, organizativa o jurídica. La primera se relaciona con la complejidad interna del modelo; la segunda, con la falta de procedimientos institucionales para documentar su funcionamiento; y la tercera, con la ausencia de reglas claras sobre qué información debe revelarse. Dexe et al. (2022) muestran que incluso bajo marcos jurídicos que reconocen información significativa sobre decisiones automatizadas persisten dificultades para determinar qué nivel de detalle resulta realmente comprensible. En el sector público, esta fragmentación puede impedir que una persona identifique qué datos fueron utilizados, qué factores tuvieron mayor peso y cómo influyó el sistema en la decisión final.

La falta de comprensión también afecta el derecho a la información. La Constitución de la República del Ecuador (2008), en su artículo 18, reconoce el derecho de acceso a información generada en instituciones públicas. De manera complementaria, la Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) obliga a garantizar acceso a información pública dentro de los límites legales establecidos. Cuando una decisión incorpora algoritmos, esta obligación exige que la administración pueda explicar al menos la función del sistema, su finalidad, los criterios relevantes y el grado de intervención humana. La complejidad técnica no debería convertirse en una causa automática de inaccesibilidad informativa.

La opacidad puede afectar también el debido proceso. La Constitución de la República del Ecuador (2008), en su artículo 76, exige garantías cuando se determinan derechos y obligaciones. Si una persona desconoce por qué fue clasificada, rechazada o sometida a una determinada medida, su capacidad de defensa se reduce. Grant et al. (2025) sostienen que las obligaciones hacia quienes son objeto de decisiones automatizadas van más allá de la mera

transparencia formal y exigen condiciones que permitan comprender y cuestionar el resultado. Por ello, la administración debe asegurar que la explicación sea suficientemente clara para permitir una respuesta efectiva por parte de la persona afectada.

La opacidad también dificulta atribuir responsabilidad institucional. Cheong (2024) relaciona transparencia y rendición de cuentas con la necesidad de proteger a las personas frente a sistemas de inteligencia artificial. Si la administración no puede reconstruir cómo se produjo una decisión, resulta difícil determinar si el error provino de los datos, del diseño, de la configuración o de la intervención humana. El Código Orgánico Administrativo (2017), en su artículo 14, mantiene la actuación pública sometida al principio de juridicidad. Esto implica que la institución no puede ampararse en la complejidad técnica del sistema para evitar justificar una actuación o identificar quién responde por sus consecuencias.

Tabla 11

Formas de opacidad algorítmica y sus efectos en la decisión pública

Tipo de opacidad	Origen principal	Dificultad generada	Riesgo jurídico
Técnica	Complejidad del modelo o aprendizaje automático	Dificultad para reconstruir el razonamiento	Falta de explicación suficiente
Organizativa	Ausencia de documentación o protocolos	Desconocimiento interno del funcionamiento	Débil rendición de cuentas
Contractual	Uso de sistemas de proveedores externos	Restricción de acceso a información técnica	Dependencia tecnológica y falta de control
Informativa	Comunicación insuficiente al ciudadano	Desconocimiento de criterios relevantes	Afectación del derecho a información
Procedimental	Falta de mecanismos de revisión	Imposibilidad de cuestionar el resultado	Afectación del debido proceso
Jurídica	Ambigüedad sobre deberes de explicación	Respuestas institucionales inconsistentes	Inseguridad jurídica

Nota. La opacidad puede presentarse en varias dimensiones simultáneamente y debe evaluarse según su efecto sobre comprensión, revisión y control de la decisión pública.

La opacidad no desaparece simplemente porque la administración publique información sobre el sistema. Arnesen (2026) distingue entre el derecho a recibir información acerca de decisiones automatizadas y un derecho más amplio a obtener explicación. Esta diferencia resulta importante porque una descripción general del algoritmo puede no permitir comprender por qué una persona concreta recibió determinado resultado. La explicación útil debe identificar

factores relevantes sin exigir necesariamente la revelación íntegra del código fuente. En la práctica administrativa, el objetivo debe ser que la persona pueda reconstruir la lógica básica de la decisión y disponer de elementos suficientes para cuestionarla si considera que vulnera sus derechos.

El derecho a conocer información relevante también encuentra respaldo en la Ley Orgánica de Protección de Datos Personales (2021), cuyo artículo 20 reconoce garantías frente a valoraciones automatizadas, incluida la posibilidad de solicitar una explicación motivada y conocer criterios de valoración, tipos y fuentes de datos utilizados. Papadimitriou (2023) destaca que el derecho a explicación busca reducir la asimetría entre quienes diseñan o utilizan sistemas de inteligencia artificial y quienes soportan sus efectos. En el sector público, esta asimetría puede ser especialmente intensa porque la persona no siempre puede evitar el procedimiento ni escoger un mecanismo alternativo para relacionarse con la administración.

El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, exige medidas relacionadas con transparencia y supervisión. De manera similar, el Reglamento (UE) 2024/1689 establece en su artículo 13 requisitos de transparencia para determinados sistemas de alto riesgo. Estos instrumentos muestran que la opacidad no debe abordarse únicamente como un problema técnico, sino como una cuestión de gobernanza y derechos. La administración necesita conservar documentación suficiente, capacidades internas de comprensión y procedimientos para explicar decisiones, especialmente cuando el sistema influye de forma relevante en el ejercicio de potestades públicas.

La opacidad algorítmica representa, en definitiva, un riesgo para transparencia, debido proceso, seguridad jurídica y rendición de cuentas. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) vincula transparencia y explicabilidad con una gobernanza responsable, mientras que Peters (2023) advierte que la falta de comprensión de los sistemas de inteligencia artificial plantea problemas específicos que no pueden resolverse trasladando mecánicamente categorías propias de decisiones humanas. En la administración pública, la respuesta debe combinar documentación, explicaciones comprensibles, trazabilidad, supervisión y mecanismos de impugnación capaces de convertir una decisión técnicamente compleja en una actuación jurídicamente controlable.

4.3 Derecho a conocer el uso de sistemas automatizados

El derecho a conocer el uso de sistemas automatizados parte de una exigencia básica de transparencia: la persona debe poder identificar cuándo una decisión pública ha sido adoptada, recomendada o condicionada mediante un sistema algorítmico. La Constitución de la República del Ecuador (2008), en su artículo 18, reconoce el derecho de acceso a la información generada por entidades públicas. En contextos automatizados, este derecho comprende información sobre la existencia del sistema, su finalidad y la función que desempeña dentro del procedimiento. Sin esta información, la ciudadanía puede desconocer que una actuación aparentemente ordinaria depende de procesos automatizados capaces de influir materialmente en sus derechos.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) refuerza esta obligación al garantizar el acceso a información pública producida, administrada o custodiada por las instituciones obligadas. En entornos algorítmicos, la transparencia debe abarcar al menos la identificación del sistema utilizado, el procedimiento en el que interviene, su finalidad institucional y los criterios generales que orientan su funcionamiento. Grimmeli Khuijsen (2023) muestra que la transparencia algorítmica afecta la percepción de confiabilidad de las decisiones automatizadas. Por ello, informar sobre la utilización de estas herramientas no constituye un elemento accesorio, sino una condición para fortalecer la posibilidad de control ciudadano.

El derecho a conocer también se vincula con la protección de datos personales. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho del titular a recibir información sobre la existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. Esta disposición es especialmente relevante cuando el sistema utiliza información personal para clasificar, predecir o asignar categorías. Arnesen (2026) distingue entre el derecho a saber que existe una decisión automatizada y el derecho posterior a obtener una explicación más sustantiva. Ambas garantías son complementarias: primero debe conocerse la intervención tecnológica y luego comprenderse su incidencia concreta.

El conocimiento sobre el uso de sistemas automatizados también resulta necesario para ejercer el debido proceso. La Constitución de la República del Ecuador (2008), en su artículo 76, exige garantías cuando se determinan derechos y obligaciones. Si una persona ignora que un algoritmo influyó en su clasificación o resultado administrativo, tiene menos posibilidades de cuestionar errores, sesgos o datos incorrectos. Dexe et al. (2022) muestran que la información significativa sobre decisiones automatizadas debe ser suficiente para permitir comprensión

real. La mera indicación de que “se utilizó inteligencia artificial” no satisface necesariamente esta exigencia si no se explica qué función desempeñó dentro del procedimiento.

El derecho a conocer el uso de sistemas automatizados se relaciona, además, con la posibilidad de atribuir responsabilidad. Cuando una institución pública utiliza una herramienta desarrollada por terceros, debe seguir siendo capaz de identificar cómo intervino en la decisión y quién debía supervisarla. El Código Orgánico Administrativo (2017), en su artículo 14, mantiene toda actuación administrativa sometida al principio de juridicidad. Por ello, la administración no puede delegar su responsabilidad informativa al proveedor tecnológico. La existencia de contratos, secretos empresariales o complejidad técnica puede justificar límites específicos, pero no puede eliminar completamente el deber de informar sobre la intervención y efectos del sistema.

Tabla 12

Contenido mínimo del derecho a conocer el uso de sistemas automatizados

Elemento de información	Finalidad	Riesgo si no se informa	Fundamento jurídico principal
Existencia del sistema	Saber que intervino una herramienta automatizada	Desconocimiento del verdadero proceso decisorio	Constitución, art. 18; LOPDP, art. 12
Finalidad	Comprender para qué se utiliza	Uso tecnológico sin justificación clara	LOPDP, art. 10
Función dentro del procedimiento	Saber si clasifica, recomienda o decide	Confusión sobre el grado de intervención algorítmica	COA, art. 14
Datos utilizados	Identificar la información procesada	Imposibilidad de detectar errores	LOPDP, arts. 12 y 20
Criterios generales	Comprender los factores relevantes	Opacidad sobre la lógica aplicada	LOPDP, art. 20
Intervención humana	Conocer quién supervisa o valida	Responsabilidad difusa	Reglamento (UE) 2024/1689, art. 14
Vías de reclamación	Permitir revisión e impugnación	Indefensión	Constitución, art. 76

Nota. El derecho a conocer debe proporcionar información suficiente para identificar la intervención del sistema, comprender su función y ejercer mecanismos de revisión.

La obligación de informar también se vincula con estándares internacionales. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, exige medidas relacionadas con transparencia y supervisión en el uso de sistemas de inteligencia artificial. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) incorpora igualmente transparencia y

explicabilidad como principios esenciales. Estos instrumentos coinciden en que las personas deben poder comprender cuándo interactúan con sistemas automatizados y cómo pueden verse afectadas. La transparencia, por tanto, debe acompañar el ciclo de vida completo del sistema y no aparecer únicamente ante una reclamación.

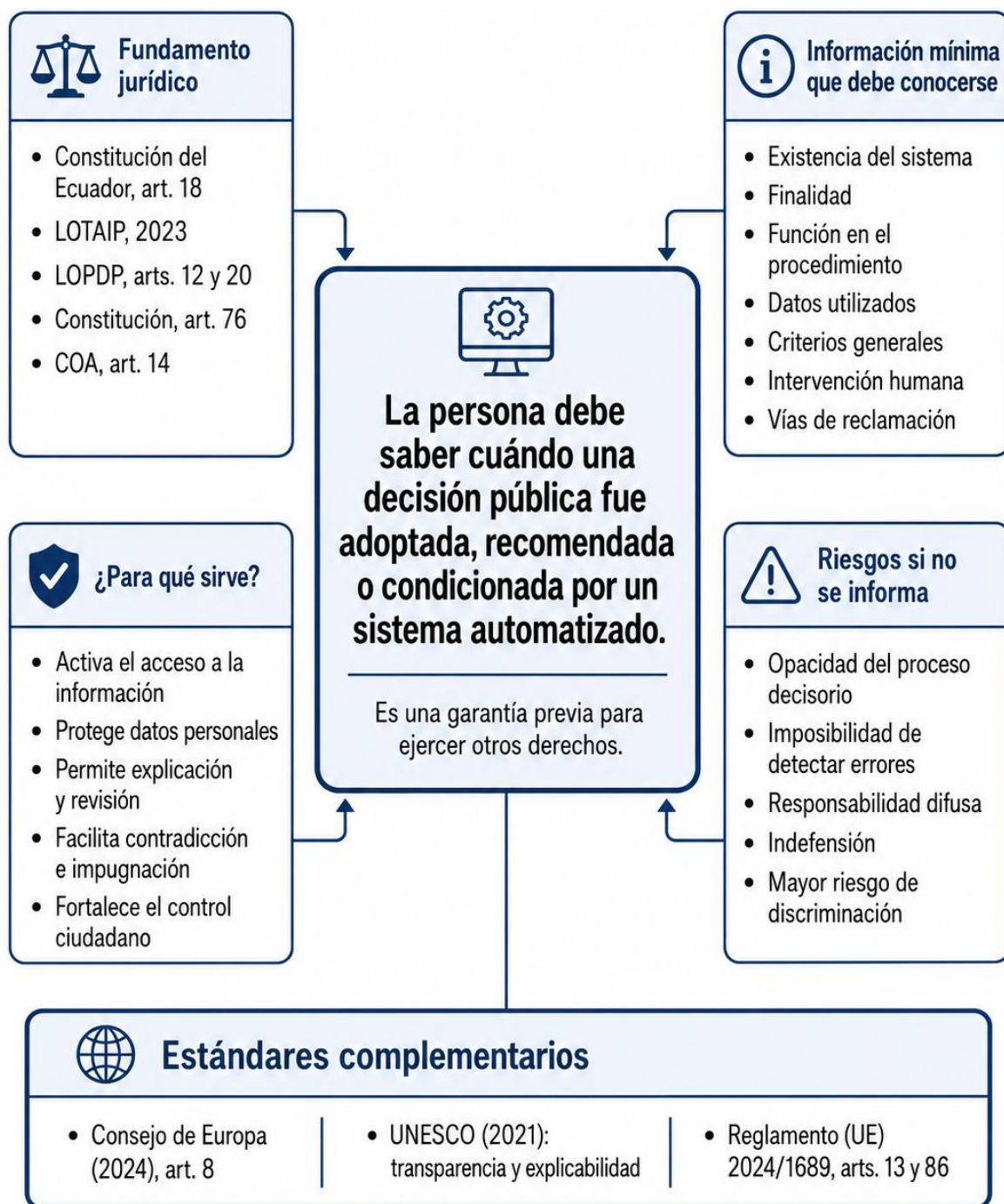
Desde el derecho comparado, el Reglamento (UE) 2024/1689 establece obligaciones específicas de transparencia. Su artículo 13 exige que determinados sistemas de alto riesgo sean suficientemente transparentes para permitir una interpretación adecuada de sus resultados, mientras que el artículo 86 contempla, en ciertos supuestos, el derecho de las personas afectadas a obtener explicaciones sobre decisiones individuales. Estas disposiciones muestran que conocer la existencia de la automatización es solo una primera capa de transparencia. La administración debe avanzar hacia información que permita comprender el papel del sistema y los elementos principales que influyeron en la decisión.

El derecho a conocer también cumple una función preventiva frente a la discriminación. Si las personas ignoran que una decisión fue asistida por un algoritmo, resulta más difícil detectar patrones de trato desigual. Cheong (2024) relaciona transparencia y rendición de cuentas con la protección frente a sistemas de inteligencia artificial, mientras que Grant et al. (2025) sostienen que las obligaciones hacia quienes son objeto de decisiones automatizadas superan la mera publicación formal de información. La transparencia debe permitir comparar resultados, identificar errores recurrentes y activar mecanismos institucionales de revisión cuando determinados grupos resultan afectados de manera sistemáticamente desfavorable.

En definitiva, el derecho a conocer el uso de sistemas automatizados constituye una garantía previa para ejercer otros derechos. Permite activar acceso a información, protección de datos, explicación, revisión, contradicción e impugnación. La Constitución de la República del Ecuador (2008), en su artículo 18, la Ley Orgánica de Protección de Datos Personales (2021), en sus artículos 12 y 20, y los estándares internacionales sobre transparencia algorítmica ofrecen una base suficiente para exigir información significativa. Una administración automatizada compatible con derechos humanos debe evitar decisiones invisibles tecnológicamente y asegurar que la ciudadanía pueda identificar cuándo, cómo y con qué efectos intervienen los sistemas algorítmicos.

Figura 7

Derecho a conocer el uso de sistemas automatizados en la administración pública



Nota. El esquema sintetiza la información mínima que debe conocer la persona sobre la intervención de sistemas automatizados, sus fundamentos jurídicos, las garantías que permite ejercer y los riesgos derivados de la falta de transparencia.

4.4 Explicabilidad de algoritmos y decisiones administrativas

La explicabilidad de los algoritmos constituye una condición para que las decisiones administrativas automatizadas puedan ser comprendidas, revisadas y cuestionadas por las personas afectadas. No exige necesariamente revelar todos los componentes técnicos del sistema, sino proporcionar información suficiente sobre los factores relevantes que influyeron en el resultado. Papadimitriou (2023) sostiene que el derecho a explicación adquiere

importancia cuando sistemas de inteligencia artificial procesan datos y generan consecuencias jurídicas. En la administración pública, esta exigencia se relaciona con la obligación de justificar la actuación estatal, especialmente cuando una clasificación, recomendación o predicción algorítmica condiciona el reconocimiento, restricción o ejercicio de un derecho.

La explicación debe diferenciarse de la mera transparencia general del sistema. Conocer que una institución utiliza inteligencia artificial no permite necesariamente comprender por qué una persona recibió un resultado determinado. Arnesen (2026) distingue precisamente entre el derecho a información sobre decisiones automatizadas y el derecho a una explicación vinculada con la decisión concreta. Dexe et al. (2022) muestran además que proporcionar información significativa exige adaptar el contenido a las necesidades de comprensión de quienes reciben la decisión. Una explicación administrativa útil debe identificar los principales datos considerados, los criterios determinantes y la forma en que estos elementos influyeron en el resultado producido.

El ordenamiento ecuatoriano ofrece un fundamento directo para exigir explicaciones frente a valoraciones automatizadas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a solicitar una explicación motivada sobre decisiones basadas única o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. Asimismo, permite conocer los criterios de valoración, los tipos y fuentes de datos utilizados y presentar observaciones. Esta disposición impide que una autoridad responda únicamente que el resultado fue generado por un sistema, pues debe poder explicar los elementos relevantes que sustentaron materialmente la valoración realizada.

La explicabilidad se relaciona también con la motivación de las decisiones públicas. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal l, dispone que las resoluciones de los poderes públicos deben estar motivadas y que no existe motivación cuando no se enuncian las normas o principios jurídicos aplicables ni se explica su pertinencia respecto de los antecedentes de hecho. En una decisión automatizada, esta garantía exige traducir el resultado algorítmico a razones jurídicamente comprensibles. Una puntuación, porcentaje o categoría de riesgo no sustituye la obligación institucional de establecer la relación entre hechos, normas aplicables y decisión adoptada.

La complejidad técnica puede limitar la posibilidad de ofrecer una reconstrucción completa del funcionamiento interno de ciertos modelos, pero no elimina la obligación de proporcionar

razones suficientes. Peters (2023) advierte que la opacidad de la inteligencia artificial presenta características particulares y que no debe equipararse automáticamente con la dificultad de comprender decisiones humanas. Grant et al. (2025) sostienen que las obligaciones hacia las personas sometidas a decisiones automatizadas superan la transparencia formal. En el ámbito administrativo, la explicación debe orientarse a permitir que la persona determine si existen datos incorrectos, criterios improcedentes, errores o fundamentos que puedan ser objeto de contradicción.

Tabla 13

Elementos de explicabilidad en las decisiones administrativas automatizadas

Elemento explicativo	Contenido requerido	Función jurídica	Fundamento principal
Existencia de automatización	Indicación de que intervino un sistema	Identificar la naturaleza del procedimiento	LOPDP, art. 12
Datos relevantes	Información utilizada para generar el resultado	Detectar errores o usos indebidos	LOPDP, art. 20
Criterios de valoración	Factores principales considerados	Comprender la lógica aplicada	LOPDP, art. 20
Resultado algorítmico	Clasificación, puntuación o recomendación generada	Identificar la incidencia tecnológica	LOPDP, art. 20
Fundamentación jurídica	Normas y principios aplicados al caso	Cumplir la exigencia de motivación	Constitución, art. 76.7.1
Intervención humana	Identificación de revisión o validación	Determinar responsabilidad institucional	Reglamento (UE) 2024/1689, art. 14
Vía de impugnación	Procedimiento para cuestionar la decisión	Garantizar defensa y revisión	Constitución, art. 76

Nota. La explicación debe permitir comprender los factores relevantes del resultado automatizado y su relación con la fundamentación jurídica de la decisión administrativa.

La explicabilidad también facilita el ejercicio del derecho de defensa. El artículo 76 de la Constitución de la República del Ecuador (2008) exige garantías de debido proceso cuando se determinan derechos y obligaciones. Una persona difícilmente puede controvertir una decisión si desconoce los elementos que determinaron el resultado. Bayamlıoğlu (2022) destaca que el derecho a impugnar decisiones automatizadas requiere algo más que una explicación abstracta del funcionamiento tecnológico. La información debe permitir formular objeciones concretas, aportar datos correctivos y cuestionar criterios aplicados. La explicación funciona así como

presupuesto para convertir la revisión administrativa o judicial en un mecanismo efectivo y no meramente formal.

Los estándares internacionales avanzan en la misma dirección. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, exige medidas relacionadas con transparencia y supervisión de sistemas de inteligencia artificial. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) incorpora la transparencia y explicabilidad entre los principios necesarios para proteger derechos humanos durante el ciclo de vida de estos sistemas. Estos instrumentos muestran que una explicación adecuada debe responder al contexto y a las consecuencias de la decisión, especialmente cuando la administración emplea inteligencia artificial en procedimientos que afectan directamente la situación jurídica de las personas.

Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 13 requisitos de transparencia para sistemas de inteligencia artificial de alto riesgo y, en su artículo 86, reconoce bajo determinadas condiciones el derecho a obtener explicaciones sobre decisiones individuales basadas en sus resultados. Estas disposiciones reflejan una tendencia hacia explicaciones orientadas al impacto concreto de los sistemas. Custers y Heijne (2022) relacionan el acceso a información sobre decisiones automatizadas con la posibilidad de ejercer derechos posteriores. Para la administración pública, esto supone conservar documentación suficiente para explicar no solo cómo funciona una herramienta, sino cómo influyó en una decisión particular.

La explicabilidad convierte la automatización en una actuación susceptible de control jurídico. No pretende exigir que cada ciudadano comprenda la arquitectura matemática del modelo, sino que pueda conocer por qué recibió determinado resultado y qué elementos puede cuestionar. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, y la Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal l, proporcionan una base interna para esta exigencia. La administración debe conservar capacidad técnica e institucional para traducir los resultados algorítmicos a razones comprensibles, jurídicamente fundamentadas y susceptibles de revisión cuando afecten derechos o intereses legítimos.

4.5 Motivación de los actos administrativos automatizados

La motivación constituye una exigencia central de validez y control de los actos administrativos, independientemente de que la decisión haya sido elaborada total o parcialmente mediante sistemas automatizados. La Constitución de la República del Ecuador

(2008), en su artículo 76, numeral 7, literal l, exige que las resoluciones de los poderes públicos expresen las normas o principios jurídicos en que se fundan y expliquen su pertinencia respecto de los antecedentes de hecho. En consecuencia, una decisión automatizada no puede limitarse a comunicar un resultado, una puntuación o una categoría; debe ofrecer razones comprensibles que permitan identificar por qué la administración adoptó esa conclusión.

La motivación de un acto automatizado exige reconstruir la relación entre hechos, datos, criterios algorítmicos y normas aplicables. El Código Orgánico Administrativo (2017), en su artículo 100, establece que la motivación debe identificar la norma jurídica aplicable, calificar los hechos relevantes y explicar la pertinencia del régimen jurídico invocado. Esta exigencia resulta particularmente importante cuando un sistema interviene en la valoración de información. La administración debe poder demostrar qué datos fueron considerados, cómo fueron interpretados y de qué manera influyeron en la decisión. La mera referencia a un resultado tecnológico no satisface por sí misma la obligación de motivación administrativa.

La utilización de inteligencia artificial puede dificultar la motivación cuando los modelos generan resultados difíciles de interpretar. Peters (2023) advierte que la opacidad algorítmica plantea problemas específicos porque la lógica computacional no siempre puede trasladarse de manera directa a razones comprensibles. Sin embargo, esta dificultad técnica no elimina la obligación jurídica de justificar la decisión. La institución debe contar con mecanismos que permitan traducir el funcionamiento relevante del sistema a términos jurídicos y administrativos. Si la propia administración no puede explicar por qué un algoritmo produjo determinado resultado, se debilita la posibilidad de controlar la legalidad y racionalidad de la actuación pública.

La motivación también exige diferenciar entre recomendación algorítmica y decisión administrativa. Un sistema puede sugerir una clasificación, una puntuación de riesgo o una prioridad, pero la autoridad sigue obligada a justificar por qué acepta o rechaza esa recomendación. Alon-Barkat y Busuioc (2023) muestran que las recomendaciones algorítmicas pueden influir significativamente en el comportamiento de los funcionarios públicos. Por ello, la motivación debe dejar constancia de la intervención humana y del papel que desempeñó el sistema. La decisión final no puede presentarse como inevitable simplemente porque una herramienta tecnológica haya generado una determinada recomendación dentro del procedimiento.

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, refuerza esta exigencia al reconocer el derecho a solicitar una explicación motivada frente a decisiones basadas única o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La norma permite además conocer criterios de valoración, tipos y fuentes de datos utilizados y formular observaciones. Esta disposición conecta directamente la motivación con la protección de datos y el derecho de defensa. La persona afectada necesita comprender qué información influyó en la decisión para poder cuestionar errores, sesgos o inferencias incorrectas utilizadas por el sistema.

La motivación de actos automatizados también se relaciona con el principio de juridicidad. El Código Orgánico Administrativo (2017), en su artículo 14, establece que la actuación administrativa debe someterse a la Constitución, los instrumentos internacionales, la ley, los principios y la jurisprudencia aplicable. Por tanto, un algoritmo no puede introducir criterios que carezcan de respaldo jurídico ni sustituir la interpretación normativa que corresponde a la autoridad competente. La motivación debe demostrar que la decisión se encuentra fundada en normas aplicables y no únicamente en correlaciones estadísticas o patrones predictivos. La tecnología puede apoyar el análisis, pero no reemplazar el fundamento jurídico necesario.

La ausencia de motivación suficiente puede afectar directamente el derecho de defensa. La Constitución de la República del Ecuador (2008), en su artículo 76, garantiza el debido proceso cuando se determinan derechos y obligaciones. Bayamlıoğlu (2022) sostiene que el derecho a impugnar decisiones automatizadas requiere información suficiente para cuestionar de manera efectiva el resultado. Si la persona desconoce qué elementos fueron determinantes, la impugnación se vuelve meramente formal. La motivación debe permitir identificar errores fácticos, criterios improcedentes o usos inadecuados de datos, de modo que la persona pueda formular objeciones concretas y solicitar revisión administrativa o judicial cuando corresponda.

La motivación también cumple una función de control institucional y de rendición de cuentas. Cheong (2024) vincula transparencia y responsabilidad con la necesidad de que los sistemas de inteligencia artificial sean auditables y comprensibles. En la administración pública, una decisión motivada permite determinar quién intervino, qué sistema fue utilizado, qué datos se procesaron y qué criterios influyeron en el resultado. Esto facilita detectar errores estructurales y establecer responsabilidades cuando se producen afectaciones. La ausencia de motivación no solo perjudica al ciudadano; también debilita la capacidad interna de supervisar el desempeño de los sistemas automatizados utilizados por la propia institución.

Los estándares internacionales avanzan en la misma dirección. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, exige medidas de transparencia y supervisión, mientras que su artículo 14 reconoce la necesidad de recursos y garantías procesales frente a decisiones vinculadas con sistemas de inteligencia artificial. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) también vincula explicabilidad, responsabilidad y supervisión humana. Estos instrumentos refuerzan la idea de que una decisión pública automatizada debe permanecer comprensible y revisable, especialmente cuando puede producir efectos significativos sobre derechos.

Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 13 requisitos de transparencia para sistemas de alto riesgo y en su artículo 14 exige supervisión humana efectiva. Además, el artículo 86 contempla, en determinados supuestos, el derecho a obtener explicaciones sobre decisiones individuales basadas en resultados de sistemas de alto riesgo. Estas disposiciones muestran que la motivación de decisiones automatizadas no puede reducirse a una explicación técnica genérica. La administración debe vincular el funcionamiento del sistema con la decisión concreta y con las normas aplicables, de modo que el resultado pueda ser comprendido y cuestionado por la persona afectada.

En definitiva, la motivación de los actos administrativos automatizados exige articular razones jurídicas, hechos relevantes, datos utilizados, intervención algorítmica y control humano. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal l, y el Código Orgánico Administrativo (2017), especialmente en sus artículos 14 y 100, proporcionan el fundamento interno para esta obligación. La automatización no disminuye la exigencia de motivar; la hace más importante, porque la complejidad tecnológica puede ocultar criterios que inciden directamente en derechos. Una decisión pública solo resulta jurídicamente controlable cuando sus razones pueden ser identificadas, comprendidas y discutidas.

4.6 Acceso a la información sobre datos, criterios y procedimientos utilizados

El acceso a la información constituye una condición indispensable para controlar decisiones públicas apoyadas en sistemas automatizados. Una persona afectada necesita conocer qué datos fueron utilizados, qué criterios influyeron en la valoración y qué procedimiento siguió la administración antes de adoptar el resultado. La Constitución de la República del Ecuador (2008), en su artículo 18, reconoce el derecho de acceso a la información generada en entidades públicas. En entornos automatizados, esta garantía debe extenderse a la información necesaria

para comprender la intervención tecnológica, siempre respetando los límites jurídicos aplicables. La opacidad del sistema no puede convertirse en una barrera automática frente al control ciudadano.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) desarrolla el derecho constitucional de acceso a la información y establece obligaciones para las instituciones públicas respecto de la información que producen, administran o custodian. En decisiones automatizadas, la transparencia debe abarcar elementos como finalidad del sistema, procedimiento administrativo en el que interviene, criterios generales de funcionamiento y responsables institucionales. La existencia de componentes técnicos no elimina la naturaleza pública de la actuación. Cuando un algoritmo participa materialmente en una decisión estatal, la administración debe conservar documentación suficiente para explicar su utilización y permitir que las personas puedan identificar cómo influyó en el resultado obtenido.

El acceso a los datos utilizados constituye una garantía especialmente relevante cuando la decisión automatizada se sustenta en información personal. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho del titular a recibir información sobre el tratamiento, mientras que su artículo 20 permite conocer criterios de valoración, tipos y fuentes de datos utilizados en determinadas decisiones automatizadas. Custers y Heijne (2022) destacan que el acceso a esta información permite ejercer otros derechos frente a procesos automatizados. Si la persona desconoce qué datos fueron considerados, difícilmente podrá identificar errores, desactualizaciones o información utilizada fuera de contexto.

El acceso a los criterios de decisión cumple una función distinta al conocimiento de los datos. Una base de información puede ser correcta y, sin embargo, el sistema aplicar variables, pesos o umbrales que produzcan un resultado cuestionable. Arnesen (2026) distingue entre el derecho a conocer la existencia de una decisión automatizada y el derecho a obtener información más sustantiva sobre sus fundamentos. Esta diferencia resulta importante en la administración pública, porque no basta con informar que se utilizó inteligencia artificial. La persona debe poder conocer los principales factores que condicionaron el resultado y determinar si esos criterios guardan relación con la finalidad jurídica del procedimiento.

El acceso al procedimiento utilizado exige también conocer cómo interactuaron sistema y servidor público. En algunos casos, el algoritmo puede limitarse a ordenar información; en otros, puede producir recomendaciones con influencia decisiva sobre el resultado. Alon-Barkat y Busuioc (2023) muestran que las recomendaciones algorítmicas pueden influir en el

comportamiento de funcionarios públicos. Por ello, la administración debería poder explicar qué fase fue automatizada, qué margen de revisión existió y quién adoptó finalmente la decisión. Esta trazabilidad permite distinguir entre asistencia tecnológica y delegación material de la valoración, aspecto esencial para atribuir responsabilidad y determinar si existió una supervisión humana efectiva.

El Código Orgánico Administrativo (2017), en su artículo 100, exige que la motivación identifique las normas aplicables, los hechos relevantes y la pertinencia del régimen jurídico utilizado. Esta obligación se relaciona directamente con el acceso a información sobre criterios y procedimientos automatizados. Si una decisión pública se sustenta parcialmente en una clasificación algorítmica, la persona debe poder comprender cómo esa clasificación se vinculó con los hechos y con las normas utilizadas. Una puntuación o categoría tecnológica no constituye por sí misma motivación suficiente. La administración debe traducir el resultado automatizado a razones jurídicas comprensibles que permitan evaluar la legalidad de la decisión.

Los límites al acceso deben interpretarse de manera restrictiva cuando la información resulta necesaria para ejercer derechos. Warthon (2024) analiza precisamente las restricciones al acceso a decisiones de inteligencia artificial por razones de interés público y destaca la importancia del principio de proporcionalidad. En la administración pública pueden existir razones legítimas para proteger información vinculada con seguridad, confidencialidad o intereses jurídicamente tutelados. Sin embargo, estas restricciones no deberían impedir por completo que la persona conozca los elementos necesarios para comprender una decisión que la afecta. El límite debe ser adecuado, necesario y proporcional respecto de la finalidad legítima que pretende proteger.

El secreto empresarial o la propiedad intelectual de proveedores externos tampoco deberían eliminar completamente la posibilidad de control. La contratación de un sistema privado no modifica la responsabilidad jurídica de la institución pública que decide utilizarlo. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, exige medidas relacionadas con transparencia y supervisión. Este estándar refuerza la necesidad de que las administraciones mantengan acceso suficiente a la documentación de los sistemas contratados. Una institución no puede justificar la falta de explicación simplemente alegando que desconoce el funcionamiento interno de una tecnología suministrada por terceros.

Figura 8

Acceso a la información en decisiones públicas apoyadas en sistemas automatizados



Nota. El esquema sintetiza la información que debe estar disponible para comprender la intervención de sistemas automatizados, ejercer mecanismos de control y establecer los límites jurídicos aplicables al acceso.

La transparencia también se relaciona con la protección frente a decisiones arbitrarias. La Constitución de la República del Ecuador (2008), en su artículo 76, garantiza el debido proceso, mientras que el Código Orgánico Administrativo (2017), en su artículo 18, reconoce la interdicción de la arbitrariedad. El acceso a datos, criterios y procedimientos permite verificar si la decisión fue adoptada conforme a razones objetivas o si dependió de factores irrelevantes, incorrectos o discriminatorios. Dexe et al. (2022) muestran que la información significativa sobre decisiones automatizadas debe permitir una comprensión real y no limitarse a descripciones generales que no expliquen el resultado concreto.

Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 13 requisitos de transparencia para sistemas de inteligencia artificial de alto riesgo y, en su artículo 86, reconoce en determinados supuestos el derecho a obtener explicaciones sobre decisiones individuales. Estas disposiciones muestran que el acceso debe abarcar información suficiente para interpretar el resultado y conocer los elementos principales que influyeron en él. La

Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) adopta una orientación similar al vincular transparencia, explicabilidad y responsabilidad. Ambas referencias refuerzan la necesidad de que los sistemas utilizados por autoridades sean jurídicamente comprensibles y auditables.

El acceso a información sobre datos, criterios y procedimientos constituye, finalmente, una condición para ejercer defensa, impugnación y control judicial. La Constitución de la República del Ecuador (2008), en sus artículos 18 y 76, junto con la Ley Orgánica de Protección de Datos Personales (2021), especialmente en sus artículos 12 y 20, proporcionan una base interna para exigir información significativa. La transparencia debe permitir reconstruir la intervención del sistema, identificar las fuentes de datos, conocer factores relevantes y determinar quién asumió la decisión. Sin estos elementos, la automatización puede convertir actuaciones públicas formalmente legales en procesos materialmente difíciles de cuestionar, debilitando las garantías de las personas afectadas.

4.7 Transparencia algorítmica como condición para el control ciudadano y jurídico

La transparencia algorítmica constituye una condición necesaria para que la ciudadanía pueda conocer, examinar y cuestionar el uso de sistemas automatizados dentro de la administración pública. No se limita a informar que existe un algoritmo, sino que exige proporcionar datos suficientes sobre su finalidad, alcance, criterios generales y participación en el procedimiento. Grimmelikhuijsen (2023) demuestra que la transparencia influye en la confianza atribuida a las decisiones automatizadas. En el ámbito estatal, esta exigencia posee además una función jurídica, porque permite identificar si la actuación se ajusta a principios de legalidad, igualdad, proporcionalidad, protección de datos y debido proceso aplicables.

El control ciudadano encuentra fundamento directo en la Constitución de la República del Ecuador (2008), cuyo artículo 18 reconoce el derecho de acceso a la información generada en entidades públicas. Este derecho permite exigir información sobre sistemas automatizados cuando su utilización forma parte de la actividad administrativa. La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) desarrolla esta garantía y obliga a las instituciones a facilitar información pública conforme a sus disposiciones. En contextos algorítmicos, el acceso debería permitir conocer la existencia del sistema, su finalidad institucional, las etapas del procedimiento en que interviene y los responsables de su utilización.

La transparencia también es indispensable para ejercer control jurídico sobre decisiones individualizadas. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal l, exige que las resoluciones públicas estén debidamente motivadas. Cuando una herramienta algorítmica influye en la decisión, la motivación debe permitir comprender cómo se relacionaron datos, criterios automatizados, hechos y normas aplicables. Papadimitriou (2023) sostiene que la explicación constituye una garantía relevante frente al procesamiento automatizado. Una decisión que solo comunica una puntuación o clasificación tecnológica sin justificar su significado jurídico dificulta la defensa y reduce la posibilidad de revisar su legalidad material.

La transparencia algorítmica también permite detectar patrones colectivos que difícilmente pueden advertirse mediante reclamaciones individuales. Cheong (2024) vincula transparencia y rendición de cuentas con la protección frente a sistemas de inteligencia artificial. Si una institución publica o facilita información sobre funcionamiento, tasas de error, criterios y resultados agregados, la ciudadanía y los organismos de control pueden identificar posibles efectos discriminatorios o desviaciones sistemáticas. Esta dimensión resulta especialmente importante cuando un sistema se utiliza de forma masiva. La revisión de un expediente individual puede corregir un error particular, pero la transparencia estructural permite descubrir problemas repetidos que requieren modificar datos, reglas o procedimientos institucionales completos.

El control ciudadano depende también de que la información sea comprensible. Savveli et al. (2025), al analizar actitudes ciudadanas hacia la evolución desde el gobierno electrónico hacia formas de gobierno apoyadas en inteligencia artificial, muestran la importancia de la percepción y aceptación pública frente a estos sistemas. La administración no debería limitarse a publicar documentos técnicos que solo puedan interpretar especialistas. La transparencia efectiva exige información adaptada a distintos públicos, explicaciones sobre funciones y riesgos, y canales para formular observaciones. La participación ciudadana pierde contenido cuando la información existe formalmente, pero su complejidad impide comprender cómo influye la automatización en los servicios y decisiones públicas.

Tabla 14

Dimensiones de la transparencia algorítmica para el control ciudadano y jurídico

Dimensión	Información necesaria	Función de control	Fundamento principal
Existencia del sistema	Identificación del uso de automatización	Permitir conocimiento ciudadano	Constitución, art. 18

Dimensión	Información necesaria	Función de control	Fundamento principal
Finalidad	Objetivo institucional del sistema	Verificar legitimidad del uso	LOPDP, art. 10
Datos utilizados	Tipos y fuentes de información	Detectar errores o usos indebidos	LOPDP, arts. 12 y 20
Criterios generales	Factores relevantes y lógica funcional	Examinar racionalidad y posible sesgo	LOPDP, art. 20
Motivación	Relación entre hechos, algoritmo y norma	Controlar legalidad de la decisión	Constitución, art. 76.7.1
Supervisión humana	Intervención y responsabilidad de funcionarios	Identificar responsables	Reglamento (UE) 2024/1689, art. 14
Resultados y auditoría	Tasas de error y efectos diferenciados	Detectar problemas estructurales	UNESCO, 2021; Consejo de Europa, 2024

Nota. La transparencia algorítmica debe permitir tanto el examen de decisiones individuales como la supervisión general de los sistemas utilizados por instituciones públicas.

El control jurídico requiere además trazabilidad suficiente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a obtener explicación motivada, conocer criterios de valoración y acceder a información sobre tipos y fuentes de datos utilizados en determinadas decisiones automatizadas. Arnesen (2026) diferencia el derecho a recibir información sobre automatización del derecho a una explicación específica sobre la decisión. Esta distinción resulta relevante porque el control jurídico no puede ejercerse únicamente con información general. La persona afectada necesita reconstruir cómo influyeron los datos y criterios del sistema en su caso concreto para formular una impugnación fundada.

Los organismos públicos también deben conservar capacidad interna para supervisar los sistemas que utilizan. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 8, establece exigencias relacionadas con transparencia y supervisión. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 13 requisitos de transparencia para sistemas de alto riesgo y en su artículo 14 mecanismos de supervisión humana. Estas disposiciones muestran que la transparencia no debe depender únicamente de solicitudes ciudadanas. La institución necesita documentación, registros y procedimientos internos que permitan auditar el funcionamiento y responder por sus efectos.

La transparencia también cumple una función preventiva frente a decisiones arbitrarias. El Código Orgánico Administrativo (2017), en su artículo 18, reconoce el principio de interdicción de la arbitrariedad, mientras que su artículo 100 establece requisitos de motivación

del acto administrativo. Cuando la administración utiliza algoritmos, estos principios exigen que los criterios tecnológicos puedan conectarse con razones jurídicas verificables. Peters (2023) advierte que la opacidad de los sistemas de inteligencia artificial presenta problemas distintos de la dificultad propia de las decisiones humanas. Por ello, la administración necesita mecanismos específicos para traducir resultados computacionales a fundamentos comprensibles y susceptibles de revisión administrativa o judicial.

La transparencia algorítmica constituye, finalmente, un requisito para mantener la responsabilidad democrática y jurídica de la administración pública. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) vincula transparencia, explicabilidad y responsabilidad durante el ciclo de vida de estos sistemas. En Ecuador, esta orientación se articula con los artículos 18 y 76 de la Constitución y con las obligaciones establecidas por la normativa de transparencia y protección de datos. Una administración automatizada solo puede permanecer sometida a control efectivo cuando permite conocer los sistemas que utiliza, comprender sus efectos, identificar responsables y activar mecanismos de revisión frente a posibles vulneraciones de derechos.

Capítulo 5

Garantías jurídicas y reparación de derechos vulnerados

María Lorena Segura Andrade



5.1 Debido proceso frente a decisiones públicas automatizadas

El debido proceso constituye una garantía esencial frente a decisiones públicas automatizadas porque asegura que la incorporación de algoritmos no reduzca las posibilidades de conocer, cuestionar y revisar la actuación administrativa. La Constitución de la República del Ecuador (2008), en su artículo 76, establece que en todo proceso en el que se determinen derechos y obligaciones deben observarse las garantías correspondientes. Esta exigencia mantiene plena vigencia cuando una decisión se apoya en inteligencia artificial. La automatización puede modificar la forma en que se analizan los hechos, pero no puede eliminar las garantías de defensa, contradicción, motivación y revisión que protegen a las personas.

Una primera exigencia del debido proceso consiste en que la persona conozca que un sistema automatizado intervino en la decisión. Si la participación algorítmica permanece oculta, resulta difícil determinar qué elementos deben cuestionarse o qué información debe solicitarse. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho a recibir información sobre la existencia de valoraciones y decisiones automatizadas. Esta transparencia inicial permite identificar la naturaleza del procedimiento y activar otras garantías. El conocimiento de la automatización no representa una formalidad informativa, sino una condición necesaria para que la persona pueda ejercer efectivamente sus derechos frente a la administración.

El derecho de defensa exige además conocer los elementos que sustentaron el resultado. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce garantías frente a determinadas decisiones basadas única o parcialmente en valoraciones automatizadas, incluyendo la posibilidad de solicitar una explicación motivada, conocer criterios de valoración, identificar tipos y fuentes de datos utilizados y formular observaciones. Estas facultades permiten cuestionar información incorrecta, criterios improcedentes o inferencias que no representen adecuadamente la situación individual. Bayamlıoğlu (2022) destaca que la posibilidad de impugnar una decisión automatizada requiere mecanismos materiales de contradicción y no únicamente transparencia formal sobre la existencia del sistema.

La motivación constituye otra garantía indispensable del debido proceso. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal 1, exige que las resoluciones públicas expresen las normas o principios aplicables y expliquen su pertinencia respecto de los hechos. En decisiones automatizadas, esta obligación exige relacionar el resultado algorítmico con los antecedentes del caso y con el fundamento jurídico

correspondiente. Fischman-Afori (2025) plantea la relevancia de incorporar el debido proceso desde el propio diseño de los sistemas de inteligencia artificial. Esta perspectiva permite entender que la motivación debe ser considerada desde la configuración tecnológica y no únicamente después de producirse una controversia.

El debido proceso también requiere que exista una intervención humana capaz de revisar efectivamente el resultado cuando la decisión pueda afectar derechos. La presencia nominal de un funcionario no garantiza por sí sola supervisión real. Green (2022) advierte que las políticas que exigen supervisión humana pueden resultar insuficientes cuando quienes revisan dependen excesivamente de recomendaciones algorítmicas. Alon-Barkat y Busuioc (2023) muestran igualmente que el asesoramiento automatizado puede influir en la conducta de los servidores públicos. Por ello, la revisión humana debe permitir apartarse del resultado, evaluar las particularidades del caso y corregir errores antes de que la decisión produzca consecuencias jurídicas.

La posibilidad de controvertir los datos utilizados es igualmente necesaria. Un sistema automatizado puede operar correctamente desde el punto de vista técnico y, sin embargo, generar una decisión injusta debido a información incompleta, incorrecta o desactualizada. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce el hábeas data para conocer, actualizar, rectificar, eliminar o anular información personal en los casos previstos constitucionalmente. Esta garantía adquiere especial importancia cuando los datos alimentan modelos utilizados repetidamente por diferentes instituciones. Sin posibilidad de corregir la información de origen, un error puede propagarse y producir sucesivas decisiones desfavorables difíciles de identificar y reparar.

La imparcialidad y la ausencia de arbitrariedad forman también parte de las condiciones del debido proceso administrativo. El Código Orgánico Administrativo (2017), en su artículo 18, reconoce el principio de interdicción de la arbitrariedad y exige que las decisiones administrativas respondan a criterios objetivos. Cuando interviene un algoritmo, esta exigencia supone verificar que las variables y reglas utilizadas tengan relación legítima con la finalidad del procedimiento. Grimmelikhuijsen y Meijer (2022) advierten que la toma de decisiones algorítmica puede generar amenazas para la legitimidad institucional. El uso tecnológico no convierte automáticamente una decisión en objetiva, pues los sistemas pueden reproducir criterios discutibles o producir efectos desproporcionados.

La revisión administrativa y judicial constituye otra garantía fundamental. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho a la tutela efectiva, imparcial y expedita de derechos e intereses. En contextos automatizados, esta garantía exige que las autoridades revisoras puedan acceder a información suficiente sobre funcionamiento, datos relevantes y criterios aplicados. Ameen et al. (2026) destacan que la revisión judicial de sistemas administrativos algorítmicos plantea desafíos relacionados con legalidad, evidencia y remedios. Una impugnación pierde eficacia cuando el órgano encargado de resolverla carece de documentación o capacidad técnica para examinar la incidencia real del sistema en la decisión cuestionada.

Los estándares internacionales refuerzan estas garantías. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 14, exige la disponibilidad de recursos accesibles y efectivos frente a vulneraciones derivadas de actividades relacionadas con sistemas de inteligencia artificial, junto con garantías procesales adecuadas. Esta disposición reconoce que la protección de derechos requiere mecanismos concretos para controvertir resultados tecnológicos. La administración debe asegurar que las personas sepan dónde reclamar, puedan presentar argumentos, obtener revisión y recibir una respuesta fundamentada. La complejidad técnica no puede transformar el derecho a impugnar en una posibilidad meramente teórica.

Desde el derecho comparado, el Reglamento (UE) 2024/1689 establece en su artículo 14 requisitos de supervisión humana para sistemas de inteligencia artificial de alto riesgo y en su artículo 86 reconoce, bajo determinadas condiciones, el derecho a obtener explicaciones sobre decisiones individuales basadas en sus resultados. Estas previsiones muestran que el debido proceso algorítmico requiere combinar información, supervisión y posibilidad de revisión. Fischman-Afori (2025) sostiene que las garantías procedimentales pueden integrarse al diseño tecnológico para fortalecer equidad y confianza. Esta aproximación resulta relevante para la administración pública, porque permite prevenir vulneraciones antes de que una decisión automatizada produzca efectos difíciles de revertir.

El debido proceso frente a decisiones públicas automatizadas exige, en definitiva, conservar todas las garantías propias de la actuación administrativa y adaptarlas a los riesgos tecnológicos. Esto implica conocimiento de la automatización, acceso a datos y criterios relevantes, motivación suficiente, contradicción, intervención humana efectiva, corrección de información, revisión e impugnación. Los artículos 75, 76 y 92 de la Constitución de la República del Ecuador (2008), junto con el artículo 20 de la Ley Orgánica de Protección de

Datos Personales (2021), proporcionan bases jurídicas para estas garantías. La innovación administrativa solo resulta legítima cuando la eficiencia tecnológica permanece subordinada a procedimientos capaces de proteger efectivamente los derechos.

Figura 9

Garantías del debido proceso frente a decisiones públicas automatizadas



Nota. El esquema sintetiza las principales garantías que deben preservarse cuando una decisión pública incorpora sistemas automatizados, incluyendo información, motivación, contradicción, revisión humana, corrección de datos e impugnación efectiva.

5.2 Derecho a la intervención y revisión humana

El derecho a la intervención y revisión humana constituye una garantía esencial frente a decisiones públicas apoyadas en sistemas automatizados. Su finalidad es evitar que una persona quede sometida a un resultado tecnológico sin posibilidad real de que un funcionario competente examine las circunstancias particulares del caso. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce garantías frente a decisiones basadas única o parcialmente en valoraciones automatizadas cuando producen efectos jurídicos o afectan derechos y libertades fundamentales. La revisión humana debe ser material y efectiva, no una validación automática del resultado producido previamente por el sistema.

La intervención humana adquiere especial importancia porque los sistemas algorítmicos pueden generar resultados técnicamente consistentes y, al mismo tiempo, inadecuados para situaciones excepcionales. Green (2022) advierte que exigir supervisión humana no garantiza por sí solo una protección efectiva cuando el funcionario acepta mecánicamente la recomendación tecnológica. Alon-Barkat y Busuioc (2023) muestran también que las recomendaciones algorítmicas pueden influir de manera considerable en las decisiones de servidores públicos. En consecuencia, la administración debe garantizar que la persona encargada de revisar posea autonomía, información suficiente y capacidad jurídica para modificar o dejar sin efecto el resultado cuando existan razones justificadas.

La revisión humana debe permitir examinar los datos utilizados, los criterios aplicados y las circunstancias individuales que el sistema pudiera haber interpretado de forma incompleta. La Constitución de la República del Ecuador (2008), en su artículo 76, garantiza el debido proceso cuando se determinan derechos y obligaciones. Esta garantía exige que la persona pueda formular observaciones y que estas sean evaluadas antes de consolidar una decisión adversa. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, contempla además la posibilidad de expresar el punto de vista del titular. De esta manera, la intervención humana debe incorporar una verdadera instancia de contradicción.

La revisión tampoco debe limitarse a comprobar que el sistema funcionó conforme a sus parámetros técnicos. El servidor público debe evaluar si el resultado es jurídicamente procedente, proporcional y compatible con los derechos de la persona. El Código Orgánico Administrativo (2017), en su artículo 14, somete la actuación administrativa al principio de juridicidad, mientras que su artículo 18 prohíbe la arbitrariedad. Estos principios impiden trasladar automáticamente al algoritmo la responsabilidad de valorar hechos y normas. La decisión final continúa siendo una actuación pública y, por tanto, debe responder a razones jurídicas que puedan ser explicadas, controladas y atribuidas a una autoridad competente.

La intervención humana exige también condiciones organizativas que hagan posible una revisión real. No basta con designar formalmente a un funcionario si este carece de capacitación, tiempo, documentación o autoridad para apartarse del resultado automatizado. Vatamanu y Tofan (2025) señalan que la integración de inteligencia artificial en la administración pública genera vulnerabilidades institucionales que requieren capacidades adecuadas de gobernanza. Una revisión efectiva necesita acceso a información relevante, conocimiento de los límites del sistema y procedimientos claros para corregir resultados. De lo

contrario, la supervisión humana puede convertirse en una formalidad que legitime decisiones previamente determinadas por la tecnología.

Tabla 15

Condiciones para una intervención y revisión humana efectiva

Condición	Contenido	Riesgo que previene	Fundamento principal
Conocimiento de la automatización	Identificar cómo intervino el sistema	Validación inconsciente del resultado	LOPDP, art. 20
Acceso a datos y criterios	Examinar información y factores utilizados	Imposibilidad de detectar errores	LOPDP, arts. 12 y 20
Autonomía del revisor	Capacidad para apartarse del resultado	Sesgo de automatización	Green (2022)
Consideración del caso individual	Evaluar circunstancias particulares	Aplicación rígida de categorías	Constitución, art. 76
Competencia jurídica	Contrastar el resultado con normas aplicables	Sustitución del juicio administrativo	COA, art. 14
Capacidad de corrección	Modificar, suspender o dejar sin efecto	Revisión meramente formal	Reglamento (UE) 2024/1689, art. 14
Registro de la revisión	Documentar quién revisó y qué decidió	Falta de trazabilidad y responsabilidad	UNESCO (2021)

Nota. La intervención humana es efectiva cuando permite examinar críticamente el resultado automatizado y modificarlo cuando resulte incorrecto, desproporcionado o jurídicamente improcedente.

La revisión humana debe producirse en un momento en que todavía sea posible evitar o corregir la afectación. Una intervención realizada únicamente después de ejecutada una decisión perjudicial puede resultar insuficiente, especialmente cuando sus efectos son inmediatos o difíciles de revertir. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) destaca la importancia de mantener supervisión humana adecuada durante el ciclo de vida de los sistemas. Desde esta perspectiva, la administración debe determinar previamente qué decisiones requieren validación humana obligatoria y cuáles pueden ser automatizadas con controles posteriores, considerando siempre la intensidad del posible impacto sobre derechos fundamentales.

El derecho comparado ofrece criterios particularmente útiles. El Reglamento (UE) 2024/1689, en su artículo 14, establece que los sistemas de inteligencia artificial de alto riesgo deben diseñarse de manera que puedan ser supervisados efectivamente por personas durante su utilización. La norma exige que quienes ejercen la supervisión comprendan las capacidades y limitaciones del sistema, puedan interpretar correctamente sus resultados y estén en

condiciones de ignorarlos, sustituirlos o detener su funcionamiento cuando corresponda. Aunque este régimen no constituye derecho ecuatoriano, proporciona un referente relevante para definir qué significa una intervención humana sustantiva en procedimientos administrativos automatizados.

La intervención humana también permite mantener claramente atribuida la responsabilidad pública. Una autoridad no debería justificar una actuación lesiva afirmando simplemente que el sistema produjo el resultado. Dragomir et al. (2026) relacionan la gobernanza de inteligencia artificial con responsabilidad institucional y protección de derechos fundamentales en la administración pública. El uso de automatización modifica las herramientas disponibles, pero no desplaza la obligación estatal de responder por las decisiones adoptadas. La revisión humana debe permitir identificar quién examinó el resultado, qué elementos consideró y por qué decidió confirmarlo o modificarlo. Esa trazabilidad resulta fundamental para posteriores controles administrativos, judiciales y ciudadanos.

En definitiva, el derecho a la intervención y revisión humana actúa como una barrera frente a la delegación absoluta de potestades públicas a sistemas automatizados. Su efectividad depende de que exista una persona competente, informada, autónoma y capaz de valorar las circunstancias particulares, escuchar al afectado y corregir el resultado. La Constitución de la República del Ecuador (2008), especialmente en su artículo 76, y la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, proporcionan bases para esta garantía. La supervisión humana solo cumple su función cuando representa una verdadera instancia decisoria y no una simple confirmación del resultado algorítmico.

5.3 Derecho de impugnación de decisiones automatizadas

El derecho de impugnación constituye una garantía esencial frente a decisiones públicas automatizadas, porque permite cuestionar resultados que puedan contener errores, sesgos o interpretaciones incompatibles con el ordenamiento jurídico. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho a la tutela efectiva, imparcial y expedita de los derechos e intereses, mientras que el artículo 76 garantiza el debido proceso cuando se determinan derechos y obligaciones. Estas garantías mantienen plena vigencia cuando intervienen algoritmos. La utilización de inteligencia artificial no puede transformar una decisión administrativa en un resultado definitivo que quede fuera de mecanismos efectivos de contradicción y revisión.

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, establece garantías específicas frente a decisiones basadas única o parcialmente en valoraciones automatizadas cuando producen efectos jurídicos o afectan derechos y libertades fundamentales. Entre ellas se encuentran la posibilidad de solicitar una explicación motivada, presentar observaciones y requerir información sobre criterios de valoración, tipos y fuentes de datos utilizados. Estas facultades proporcionan elementos necesarios para cuestionar el resultado obtenido. Bayamlıoğlu (2022) señala que el derecho a controvertir decisiones automatizadas posee un alcance que supera la mera explicación, pues requiere mecanismos capaces de producir una revisión efectiva de la situación individual.

La impugnación exige que la persona conozca suficientemente las razones de la decisión. No puede cuestionarse de manera efectiva un resultado cuando se desconocen los datos, criterios o inferencias que lo produjeron. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal 1, exige motivación de las resoluciones de los poderes públicos. Esta garantía adquiere particular relevancia cuando la decisión incorpora una puntuación, clasificación o recomendación algorítmica. Arnesen (2026) diferencia la información general sobre automatización de la explicación relativa a una decisión específica. La segunda proporciona bases más adecuadas para identificar los aspectos susceptibles de controversia o corrección.

El derecho de impugnación también supone que la revisión sea realizada por una instancia capaz de evaluar críticamente el resultado automatizado. Una reconsideración que reproduzca exactamente el mismo procedimiento algorítmico, sin examinar las objeciones formuladas, difícilmente constituye una garantía efectiva. Green (2022) advierte que la presencia humana puede resultar insuficiente cuando existe dependencia excesiva de la recomendación tecnológica. Por ello, quien revise una decisión debe disponer de autoridad para modificarla, acceso a la información relevante y capacidad para considerar circunstancias que el sistema no incorporó adecuadamente. La revisión debe constituir un nuevo examen y no una simple confirmación tecnológica del resultado inicial.

La posibilidad de cuestionar los datos utilizados representa otra dimensión fundamental de la impugnación. Una decisión puede resultar incorrecta porque el sistema procesó información desactualizada, incompleta o atribuida erróneamente a la persona. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce el hábeas data como mecanismo para conocer la existencia y utilización de información personal, así como solicitar su actualización, rectificación, eliminación o anulación en los casos correspondientes. Cuando

esos datos alimentan sistemas automatizados, corregirlos puede resultar indispensable para revisar tanto la decisión concreta como futuras actuaciones que utilicen la misma información dentro de procesos administrativos.

El derecho de impugnación adquiere especial complejidad cuando las decisiones dependen de perfiles o inferencias producidos por sistemas algorítmicos. Metikos (2024) analiza la explicación y contestación de sistemas de perfilamiento y muestra que la posibilidad de cuestionar estos mecanismos requiere comprender cómo determinadas características o inferencias influyen en el resultado. Esta problemática también aparece fuera del ámbito judicial cuando las administraciones clasifican personas según riesgo, prioridad o elegibilidad. La impugnación debe permitir cuestionar no solamente datos objetivos incorrectos, sino también inferencias, categorías y relaciones estadísticas cuya aplicación al caso individual pueda resultar inadecuada, desproporcionada o jurídicamente injustificada.

La revisión judicial constituye una garantía complementaria cuando los mecanismos administrativos no permiten corregir la afectación. Ameen et al. (2026) advierten que el control judicial de sistemas administrativos algorítmicos plantea problemas específicos relacionados con legalidad, prueba y determinación de remedios. El artículo 75 de la Constitución de la República del Ecuador (2008) exige tutela judicial efectiva, lo que implica que la complejidad tecnológica no debe impedir que los órganos jurisdiccionales examinen una decisión. Para ello, la administración necesita conservar registros, documentación y evidencia suficiente sobre datos, funcionamiento del sistema, intervención humana y fundamentos empleados durante el procedimiento que originó la controversia.

La impugnación debe ser accesible también desde el punto de vista material. Un procedimiento excesivamente técnico puede dificultar que las personas identifiquen qué deben cuestionar o qué pruebas necesitan aportar. Fischman-Afori (2025) plantea que las garantías del debido proceso deberían integrarse desde el diseño de los sistemas de inteligencia artificial. Aplicada a la administración pública, esta perspectiva implica configurar mecanismos que faciliten solicitar revisión, aportar información adicional, señalar errores y recibir respuestas comprensibles. El ejercicio de un derecho no debe depender de conocimientos avanzados sobre programación o modelos estadísticos. Corresponde a la institución traducir la complejidad tecnológica a procedimientos jurídicamente accesibles para la ciudadanía.

Los estándares internacionales refuerzan esta orientación. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho

(2024), en su artículo 14, exige recursos accesibles y efectivos frente a vulneraciones de derechos derivadas de actividades relacionadas con sistemas de inteligencia artificial. Esta garantía comprende la necesidad de disponer de información pertinente para que las personas puedan cuestionar las decisiones que las afectan. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021) también vincula responsabilidad, supervisión y mecanismos de reparación. Estos estándares muestran que la posibilidad de impugnar constituye una condición central de una gobernanza algorítmica respetuosa de derechos.

Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 86, bajo las condiciones previstas en esa disposición, la posibilidad de obtener explicaciones sobre determinadas decisiones individuales basadas en resultados de sistemas de inteligencia artificial de alto riesgo. Esta información puede facilitar posteriormente su cuestionamiento. Asimismo, el artículo 14 establece requisitos de supervisión humana para sistemas de alto riesgo. La combinación de explicación y revisión muestra que la protección efectiva no termina cuando la persona recibe información sobre el funcionamiento del sistema. Deben existir mecanismos institucionales capaces de reconsiderar el resultado y adoptar una decisión diferente cuando la valoración automatizada resulte incorrecta o improcedente.

El derecho de impugnación de decisiones automatizadas constituye, en definitiva, una garantía contra la irreversibilidad de los resultados algorítmicos. Su ejercicio requiere información suficiente, motivación, acceso a datos y criterios relevantes, revisión humana efectiva y posibilidad de acudir a mecanismos administrativos o judiciales. Los artículos 75, 76 y 92 de la Constitución de la República del Ecuador (2008), junto con el artículo 20 de la Ley Orgánica de Protección de Datos Personales (2021), ofrecen fundamentos para estas garantías. La automatización pública solo resulta compatible con los derechos humanos cuando sus resultados permanecen abiertos a contradicción, revisión, corrección y eventual reparación.

5.4 Control administrativo y judicial de los sistemas algorítmicos

El control administrativo y judicial de los sistemas algorítmicos constituye una garantía necesaria para asegurar que la automatización pública permanezca sometida al ordenamiento jurídico. La incorporación de inteligencia artificial no modifica el principio según el cual toda actuación estatal debe poder ser revisada, corregida y, cuando corresponda, anulada. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho a la tutela efectiva, imparcial y expedita, mientras que el artículo 76 garantiza el debido proceso.

Estas disposiciones permiten afirmar que las decisiones asistidas por algoritmos no pueden quedar fuera de mecanismos institucionales capaces de controlar su legalidad y sus efectos.

El control administrativo debe comenzar dentro de la propia institución que utiliza el sistema. La administración necesita mecanismos para revisar periódicamente los datos empleados, los criterios de funcionamiento, los resultados producidos y la intervención de los funcionarios responsables. El Código Orgánico Administrativo (2017), en su artículo 14, establece el principio de juridicidad, lo que obliga a que toda actuación pública se ajuste a la Constitución, instrumentos internacionales, leyes y demás fuentes aplicables. Esta exigencia implica que los sistemas algorítmicos deben ser evaluados no solo desde su rendimiento técnico, sino también desde su compatibilidad con los derechos y principios que rigen la actividad administrativa.

El control interno requiere además trazabilidad. Una institución debe poder reconstruir qué versión del sistema fue utilizada, qué datos ingresaron, qué resultado produjo y qué funcionario intervino antes de adoptar la decisión. Cheong (2024) relaciona la transparencia algorítmica con la rendición de cuentas y la posibilidad de identificar responsabilidades. Sin registros suficientes, la administración puede encontrar dificultades para determinar si un problema se originó en los datos, en el modelo, en su configuración o en una decisión humana posterior. La trazabilidad constituye, por tanto, una condición técnica y jurídica para que el control administrativo pueda producir correcciones efectivas.

La auditoría algorítmica representa otra herramienta relevante de control. Su función consiste en examinar el comportamiento del sistema, detectar errores recurrentes, identificar efectos discriminatorios y verificar que los resultados se mantengan dentro de los parámetros jurídicos establecidos. Dragomir et al. (2026) destacan la relación entre gobernanza de inteligencia artificial, responsabilidad y resiliencia institucional en la administración pública. Desde esta perspectiva, la auditoría no debe limitarse a comprobar precisión estadística, sino incluir criterios relacionados con derechos fundamentales, legalidad, transparencia y proporcionalidad. Un sistema técnicamente eficiente puede seguir siendo jurídicamente problemático si produce impactos incompatibles con las obligaciones públicas.

El control administrativo también debe permitir suspender o modificar un sistema cuando existan riesgos significativos. El principio de prevención exige que las instituciones no esperen a que se acumulen daños para intervenir. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 42, contempla evaluaciones de impacto cuando el tratamiento pueda generar alto riesgo para derechos y libertades. Este enfoque preventivo puede extenderse al

control de sistemas automatizados utilizados en decisiones públicas. Si una evaluación revela errores sistemáticos, discriminación o uso desproporcionado de datos, la administración debe contar con facultades y procedimientos para corregir, limitar o detener temporalmente su utilización.

El control judicial adquiere relevancia cuando una persona considera que una decisión automatizada vulneró sus derechos o cuando los mecanismos administrativos resultan insuficientes. Ameen et al. (2026) advierten que la revisión judicial de sistemas administrativos algorítmicos plantea desafíos particulares relacionados con legalidad, prueba y remedios. Los jueces necesitan información suficiente para comprender el papel del sistema en la decisión impugnada. Esto exige que la administración conserve documentación, registros, explicaciones y evidencia sobre datos y criterios relevantes. De lo contrario, la complejidad técnica puede transformarse en una barrera que dificulte el ejercicio efectivo de la tutela judicial.

La carga probatoria representa uno de los principales desafíos del control judicial. Una persona puede identificar un resultado perjudicial sin tener acceso al funcionamiento interno del sistema que lo produjo. Esta asimetría informativa puede dificultar demostrar la existencia de errores o sesgos. Metikos (2024), al estudiar la explicación y contestación de sistemas de perfilamiento, muestra que la posibilidad de cuestionar decisiones automatizadas depende de disponer de información suficiente sobre los factores relevantes. En estos casos, los tribunales pueden necesitar mecanismos procesales capaces de exigir documentación a la administración y permitir análisis técnicos independientes cuando la controversia dependa del funcionamiento de un sistema algorítmico.

El hábeas data constituye una herramienta particularmente relevante cuando la controversia se relaciona con datos personales utilizados por sistemas automatizados. La Constitución de la República del Ecuador (2008), en su artículo 92, permite conocer la existencia, uso, finalidad, origen y destino de información personal, así como solicitar su actualización, rectificación, eliminación o anulación en los casos previstos. La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en sus artículos 49 y 50, desarrolla esta garantía. Cuando un sistema produce decisiones a partir de información incorrecta, el control judicial puede dirigirse tanto contra el resultado administrativo como contra la base de datos que lo condicionó.

El control judicial debe evaluar también la motivación del acto. La Constitución de la República del Ecuador (2008), en su artículo 76, numeral 7, literal l, exige que las resoluciones públicas estén motivadas. Si una autoridad utiliza un resultado algorítmico sin explicar por qué

lo considera jurídicamente relevante, el acto puede quedar debilitado desde la perspectiva del debido proceso. Fischman-Afori (2025) propone incorporar garantías procedimentales desde el diseño mismo de los sistemas de inteligencia artificial. Esta perspectiva ayuda a comprender que la posibilidad de revisión judicial depende, en buena medida, de que la administración haya generado previamente registros y explicaciones suficientes.

Figura 10

Control administrativo y judicial de los sistemas algorítmicos



Nota. El esquema sintetiza los principales mecanismos de control administrativo y judicial aplicables a los sistemas algorítmicos, orientados por los principios de legalidad, transparencia, rendición de cuentas, proporcionalidad y efectividad.

El derecho comparado ofrece criterios adicionales para estructurar estos controles. El Reglamento (UE) 2024/1689 establece en su artículo 9 sistemas de gestión de riesgos para determinadas aplicaciones de alto riesgo y en su artículo 27 evaluaciones de impacto sobre derechos fundamentales en ciertos supuestos. Por su parte, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 14, exige recursos accesibles y efectivos frente a vulneraciones relacionadas con sistemas de inteligencia artificial. Estas disposiciones muestran una tendencia hacia controles preventivos, administrativos y judiciales articulados durante todo el ciclo de vida tecnológico.

El control administrativo y judicial de los sistemas algorítmicos debe entenderse, finalmente, como un sistema continuo de supervisión y responsabilidad. El control interno permite detectar riesgos y corregir fallas antes de que produzcan daños generalizados, mientras que la revisión judicial garantiza una instancia independiente cuando los derechos resultan afectados. Los artículos 75, 76 y 92 de la Constitución de la República del Ecuador (2008), junto con los principios del Código Orgánico Administrativo y la normativa de protección de datos, ofrecen bases para estos mecanismos. La automatización pública solo puede considerarse legítima cuando permanece sometida a auditoría, explicación, impugnación y control jurisdiccional efectivo.

5.5 Determinación de responsabilidad por decisiones automatizadas

La determinación de responsabilidad constituye uno de los principales desafíos jurídicos derivados del uso de sistemas automatizados en la administración pública. Cuando una decisión produce una afectación, puede resultar complejo identificar si el origen se encuentra en los datos, el diseño del algoritmo, su configuración, la actuación del proveedor o la intervención del funcionario responsable. Sin embargo, la automatización no elimina la responsabilidad institucional. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 9, establece como deber primordial del Estado respetar y hacer respetar los derechos garantizados constitucionalmente. Por ello, una herramienta tecnológica no puede convertirse en un mecanismo de exoneración estatal.

La responsabilidad debe analizarse considerando las distintas etapas del ciclo de vida del sistema. Un error puede originarse durante la selección de datos, el entrenamiento del modelo, su adquisición, implementación, actualización o utilización dentro de un procedimiento administrativo. Cheong (2024) relaciona la rendición de cuentas algorítmica con la posibilidad de identificar actores responsables y examinar las decisiones adoptadas durante el desarrollo y funcionamiento de los sistemas. En el sector público, esta perspectiva exige documentar quién autorizó su utilización, qué unidad supervisó su funcionamiento, quién interpretó el resultado y qué autoridad adoptó finalmente la decisión con efectos sobre la persona afectada.

La participación de empresas proveedoras introduce una distribución adicional de funciones, pero no elimina la responsabilidad de la administración. Una institución puede contratar el desarrollo o mantenimiento de un sistema, aunque continúa siendo responsable de justificar jurídicamente su utilización dentro de potestades públicas. Dragomir et al. (2026) destacan que la gobernanza de inteligencia artificial requiere estructuras institucionales claras de

responsabilidad. Las cláusulas contractuales deberían, por tanto, permitir acceso a documentación, auditoría y cooperación cuando se produzcan controversias. La administración no debería implementar tecnologías cuya configuración contractual le impida comprender, supervisar o explicar suficientemente los resultados utilizados para adoptar decisiones que afectan derechos ciudadanos.

La responsabilidad individual de los servidores públicos continúa siendo relevante. La Constitución de la República del Ecuador (2008), en su artículo 233, dispone que ninguna servidora ni servidor público está exento de responsabilidades por los actos realizados en el ejercicio de sus funciones o por sus omisiones. La utilización de una recomendación algorítmica no desplaza automáticamente esta regla. Alon-Barkat y Busuioc (2023) muestran que los funcionarios pueden adherirse de manera significativa a recomendaciones automatizadas. En consecuencia, quienes intervienen en procedimientos automatizados deben ejercer una valoración crítica y evitar considerar el resultado tecnológico como una justificación suficiente para adoptar una decisión potencialmente lesiva.

La asignación de responsabilidad requiere asimismo distinguir entre fallo tecnológico y deficiencia institucional. Green (2022) advierte que la supervisión humana puede resultar ineficaz cuando se configura únicamente como requisito formal. Si una organización carece de capacitación, protocolos de revisión o mecanismos para detectar errores, la responsabilidad no debería concentrarse exclusivamente en quien confirmó individualmente el resultado. También deben analizarse las decisiones institucionales relacionadas con diseño, adquisición, implantación y supervisión. La responsabilidad algorítmica exige así una perspectiva multinivel capaz de identificar tanto conductas particulares como fallas organizativas que permitieron que una herramienta defectuosa o inadecuada produjera consecuencias jurídicas.

Tabla 16

Ámbitos de responsabilidad en decisiones públicas automatizadas

Ámbito de responsabilidad	Actor involucrado	Situación que puede generar responsabilidad	Mecanismo de control
Institucional	Entidad pública	Uso de sistemas incompatibles con derechos o normas	Auditoría y control administrativo
Funcional	Servidor público	Validación irreflexiva o actuación contraria a derecho	Responsabilidad administrativa

Ámbito de responsabilidad	Actor involucrado	Situación que puede generar responsabilidad	Mecanismo de control
Tecnológica	Desarrollador o proveedor	Defectos de diseño, documentación o funcionamiento	Supervisión contractual y técnica
Datos	Responsable del tratamiento	Uso de información incorrecta, excesiva o ilegítima	LOPDP y evaluación de impacto
Supervisión	Unidad responsable	Falta de monitoreo o detección de riesgos	Control interno
Decisoria	Autoridad competente	Adopción de una resolución jurídicamente improcedente	Impugnación administrativa o judicial
Estatal	Estado	Vulneración de derechos atribuible a actuación pública	Constitución, art. 11.9

Nota. La responsabilidad debe determinarse considerando la intervención concreta de cada actor y las decisiones adoptadas durante el ciclo de vida del sistema automatizado.

La protección de datos incorpora también obligaciones relevantes para determinar responsabilidades. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, contempla la responsabilidad proactiva entre los principios aplicables al tratamiento. Esto exige que quienes manejan datos puedan demostrar la adopción de medidas orientadas al cumplimiento de la normativa. En decisiones automatizadas, esta obligación adquiere especial importancia porque la institución debe documentar cómo fueron seleccionados los datos, qué riesgos identificó y qué controles estableció. Christodoulou y Limniotis (2024) muestran que los sistemas basados en aprendizaje automático generan desafíos específicos para atribuir y demostrar cumplimiento de obligaciones relacionadas con protección de datos.

La responsabilidad debe permanecer identificable incluso cuando varios actores participan en el proceso. He y Zhang (2025) analizan los conflictos entre poder algorítmico, derechos y límites jurídicos, destacando la necesidad de estructuras de gobernanza capaces de controlar sus efectos. Desde esta perspectiva, la responsabilidad no puede quedar fragmentada hasta el punto de que ninguno de los participantes responda por el resultado final. La administración debe establecer previamente funciones, competencias y obligaciones de supervisión. Los registros de actividad, decisiones de configuración, versiones del sistema y revisiones humanas permiten reconstruir posteriormente la cadena de actuación y determinar dónde ocurrió una falla jurídicamente relevante.

Los estándares internacionales respaldan este enfoque. La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021), especialmente en sus párrafos 35 y 36, vincula

responsabilidad y rendición de cuentas con la necesidad de mantener mecanismos adecuados de supervisión durante el ciclo de vida de los sistemas. Como referencia comparada, el Reglamento (UE) 2024/1689 distribuye obligaciones entre diferentes participantes de la cadena de inteligencia artificial y establece, en su artículo 26, deberes específicos para quienes despliegan determinados sistemas de alto riesgo. Estos estándares muestran que la asignación anticipada de responsabilidades constituye una condición de gobernanza y no únicamente una respuesta posterior al daño.

La determinación de responsabilidad por decisiones automatizadas exige, finalmente, impedir que la complejidad tecnológica genere espacios de irresponsabilidad. El algoritmo carece de responsabilidad jurídica propia; la responsabilidad corresponde a personas, autoridades, instituciones y, según las circunstancias, proveedores que intervienen en su diseño, implementación o utilización. Los artículos 11, numeral 9, y 233 de la Constitución de la República del Ecuador (2008) permiten mantener la responsabilidad estatal y funcional como principios centrales. La trazabilidad, documentación y supervisión deben permitir reconstruir la cadena decisoria, atribuir consecuencias y garantizar que la innovación tecnológica permanezca sometida a mecanismos efectivos de rendición de cuentas y reparación.

5.6 Prueba del daño y de la vulneración de derechos en entornos algorítmicos

La prueba del daño en entornos algorítmicos presenta dificultades particulares porque los efectos de una decisión automatizada no siempre son visibles de manera inmediata. Una persona puede recibir una clasificación desfavorable sin conocer qué datos, inferencias o reglas produjeron el resultado. Ameen et al. (2026) señalan que la revisión de sistemas administrativos algorítmicos plantea desafíos relacionados con evidencia, legalidad y determinación de remedios. En estos casos, demostrar la vulneración exige reconstruir la cadena decisoria y establecer una conexión entre el funcionamiento del sistema y la afectación producida. La opacidad tecnológica no debería convertir el daño en jurídicamente indemostrable.

Una primera dificultad consiste en acceder a la evidencia necesaria. Los datos de entrada, registros del sistema, parámetros relevantes, versiones del modelo y decisiones de supervisión pueden encontrarse bajo control exclusivo de la administración o del proveedor tecnológico. Esta asimetría coloca a la persona afectada en una posición probatoria desfavorable. Metikos (2024) muestra que la posibilidad de cuestionar sistemas de perfilamiento depende de disponer de información suficiente sobre los factores que influyen en el resultado. Por ello, los

procedimientos administrativos y judiciales deben permitir obtener documentación técnica cuando resulte indispensable para determinar si existió una afectación jurídicamente relevante.

La prueba también puede requerir demostrar que el daño no deriva exclusivamente de un dato incorrecto, sino de una inferencia o patrón generado por el sistema. Binns y Veale (2021) explican que los procesos de perfilamiento pueden desarrollarse en varias etapas y producir efectos selectivos difíciles de identificar. Una persona puede aparecer correctamente registrada en las bases de datos y, aun así, ser clasificada de manera inadecuada mediante correlaciones estadísticas. En consecuencia, el análisis probatorio debe abarcar datos originales, transformaciones, inferencias y decisiones posteriores. Limitarse a comprobar la exactitud de la información inicial puede dejar sin examinar la verdadera fuente del perjuicio.

La Constitución de la República del Ecuador (2008), en su artículo 75, garantiza tutela efectiva, imparcial y expedita, mientras que el artículo 76 reconoce las garantías del debido proceso. Estas disposiciones exigen que las reglas probatorias no hagan imposible cuestionar una decisión automatizada. Cuando la evidencia esencial se encuentra bajo control estatal, la administración debe conservarla y facilitar su examen en los términos jurídicamente procedentes. El Código Orgánico Administrativo (2017), en su artículo 100, exige además que los actos administrativos estén debidamente motivados. Una motivación documentada facilita reconstruir los hechos, criterios y fundamentos utilizados para valorar posteriormente la existencia de una vulneración.

La prueba del daño puede adquirir una dimensión colectiva cuando un sistema produce patrones recurrentes de perjuicio. Wang et al. (2024) muestran que la discriminación algorítmica puede manifestarse mediante efectos diferenciados que solo se hacen visibles al comparar resultados entre grupos. En estos casos, una decisión individual puede parecer aislada, mientras que el análisis agregado revela un patrón sistemático. Por ello, la prueba puede requerir estadísticas, tasas de error, resultados desagregados y auditorías. La identificación de un impacto colectivo no elimina la necesidad de examinar el caso concreto, pero permite contextualizarlo y determinar si la afectación forma parte de una falla estructural del sistema.

Tabla 17

Elementos probatorios para acreditar daños y vulneraciones en decisiones algorítmicas

Elemento probatorio	Utilidad	Dificultad frecuente	Fuente posible
Datos de entrada	Verificar información utilizada	Acceso restringido o fragmentado	Expediente y bases institucionales
Inferencias y perfiles	Identificar clasificaciones derivadas	Opacidad del modelo	Registros y documentación técnica
Criterios y parámetros	Analizar factores relevantes	Complejidad técnica	Documentación del sistema
Registros de ejecución	Reconstruir el proceso concreto	Conservación insuficiente	Logs y trazabilidad institucional
Intervención humana	Determinar supervisión y responsabilidad	Falta de documentación	Expediente administrativo
Resultados comparados	Detectar efectos sistemáticos	Ausencia de datos desagregados	Auditorías y estadísticas
Informes periciales	Interpretar evidencia técnica	Necesidad de conocimiento especializado	Peritaje independiente

Nota. La prueba debe permitir reconstruir la relación entre datos, funcionamiento del sistema, decisión adoptada y afectación concreta o colectiva de derechos.

La carga probatoria debe analizarse teniendo en cuenta la desigualdad informativa existente entre la persona y la institución que utiliza el sistema. Warthon (2024) advierte que las restricciones de acceso a información sobre inteligencia artificial deben justificarse mediante criterios de proporcionalidad. Cuando el conocimiento técnico necesario para probar el daño permanece exclusivamente en manos de la administración, una interpretación excesivamente restrictiva del acceso puede impedir una defensa efectiva. Esto no significa revelar indiscriminadamente toda la arquitectura del sistema, sino proporcionar la información necesaria para que la persona y la autoridad revisora puedan examinar los elementos relevantes de la decisión cuestionada.

La protección de datos también aporta mecanismos probatorios importantes. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, permite solicitar explicación motivada y conocer criterios de valoración, tipos y fuentes de datos utilizados en determinadas decisiones automatizadas. Asimismo, el artículo 42 prevé evaluaciones de impacto frente a tratamientos de alto riesgo. Estos documentos pueden convertirse en evidencia relevante para determinar si la institución identificó previamente riesgos y adoptó medidas adecuadas. Thomaidou y Limniotis (2025) destacan precisamente la utilidad de las evaluaciones de impacto para examinar consecuencias sobre protección de datos y derechos fundamentales derivadas del uso de inteligencia artificial.

El análisis probatorio debe considerar también los daños que se acumulan progresivamente. Teo (2025) utiliza la noción de violencia lenta para explicar cómo determinados efectos de la inteligencia artificial sobre los derechos pueden desarrollarse de manera gradual y difícil de percibir. En la administración pública, una persona podría sufrir reiteradas exclusiones, menores oportunidades o decisiones desfavorables vinculadas con una misma clasificación algorítmica sin que exista un único evento claramente identificable. La prueba, por tanto, puede requerir reconstruir una secuencia de decisiones y analizar cómo una inferencia persistente condicionó diferentes actuaciones públicas a lo largo del tiempo.

La prueba de vulneraciones en entornos algorítmicos exige, finalmente, sistemas que conserven evidencia suficiente para permitir control posterior. Sin trazabilidad, documentación y registros, resulta difícil determinar causalidad, responsabilidad y reparación. La Constitución de la República del Ecuador (2008), en sus artículos 75 y 76, exige garantías efectivas de tutela y debido proceso, mientras que la normativa de protección de datos proporciona herramientas para acceder a información relacionada con decisiones automatizadas. La administración debe diseñar sus sistemas considerando desde el inicio la posibilidad de revisión probatoria. Una tecnología que no permite reconstruir sus decisiones genera un riesgo incompatible con una actuación pública jurídicamente controlable.

5.7 Mecanismos de reparación y restitución de derechos vulnerados

La reparación constituye una consecuencia indispensable cuando una decisión pública automatizada provoca la vulneración de derechos. No basta con identificar el error o declarar que el sistema actuó de manera inadecuada; es necesario restablecer, en la medida de lo posible, la situación jurídica afectada y evitar que el daño continúe produciendo efectos. La Constitución de la República del Ecuador (2008), en su artículo 11, numeral 9, establece la responsabilidad del Estado por violaciones de derechos ocasionadas por acciones u omisiones de sus funcionarios. En entornos algorítmicos, esta obligación comprende también las consecuencias derivadas del uso institucional de sistemas automatizados.

La tutela judicial efectiva proporciona una base adicional para exigir reparación. La Constitución de la República del Ecuador (2008), en su artículo 75, reconoce el derecho a acceder gratuitamente a la justicia y obtener una tutela efectiva, imparcial y expedita de derechos e intereses. Cuando una decisión automatizada produce una afectación, esta garantía exige que existan mecanismos capaces de revisar el acto, suspender sus efectos y adoptar medidas correctivas. Ameen et al. (2026) destacan que la revisión judicial de sistemas

administrativos algorítmicos plantea desafíos específicos respecto de los remedios disponibles. La respuesta jurídica debe adaptarse, por tanto, a las características particulares del daño tecnológico.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 18, establece que cuando se declara la vulneración de derechos debe ordenarse la reparación integral por el daño material e inmaterial. La norma contempla medidas orientadas a restituir el derecho, compensar consecuencias y garantizar que la vulneración no vuelva a repetirse. Este enfoque resulta especialmente pertinente frente a sistemas automatizados, porque una afectación puede prolongarse mientras el algoritmo continúe utilizando datos, perfiles o criterios incorrectos. La reparación debe intervenir no solamente sobre la decisión individual, sino también sobre los componentes tecnológicos que mantienen o reproducen el perjuicio.

La restitución constituye una de las primeras medidas que pueden adoptarse. Su objetivo consiste en devolver a la persona, en cuanto sea posible, a la situación existente antes de la vulneración. En decisiones automatizadas, esto puede implicar dejar sin efecto una clasificación, reconsiderar una solicitud, eliminar una restricción o repetir el procedimiento sin utilizar información incorrecta. La Constitución de la República del Ecuador (2008), en su artículo 92, permite mediante hábeas data solicitar actualización, rectificación, eliminación o anulación de información personal. Cuando el perjuicio proviene de datos erróneos, corregir la fuente constituye una condición necesaria para lograr una restitución efectiva.

La reparación puede requerir también corregir inferencias o perfiles producidos por el sistema. Binns y Veale (2021) explican que el perfilamiento automatizado puede desarrollarse en varias etapas y producir efectos que no derivan directamente de un único dato. Por ello, eliminar una información incorrecta puede resultar insuficiente si permanecen clasificaciones derivadas de ella. La restitución debe alcanzar, cuando corresponda, perfiles, puntuaciones o inferencias generadas a partir de información posteriormente rectificada. De otro modo, la persona podría seguir soportando decisiones desfavorables pese a haberse corregido formalmente el dato original que dio origen a la clasificación automatizada.

La compensación puede resultar necesaria cuando la restitución completa ya no es posible. Determinadas decisiones automatizadas pueden producir pérdidas económicas, retrasos en prestaciones, exclusiones indebidas o afectaciones que no desaparecen simplemente anulando el acto. La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 18, reconoce que la reparación integral puede comprender compensación por daños

materiales e inmateriales. En estos casos, la determinación del daño requiere establecer la relación entre la actuación automatizada y la consecuencia sufrida. La complejidad tecnológica no debe impedir que la persona obtenga reparación cuando exista una afectación jurídicamente demostrable atribuible a la administración.

Las garantías de no repetición resultan especialmente importantes cuando el daño proviene de una falla estructural del sistema. Si una decisión incorrecta deriva de un modelo sesgado, una base de datos defectuosa o un procedimiento institucional inadecuado, corregir únicamente el caso individual deja intacto el riesgo para otras personas. Teo (2025) advierte que los efectos de la inteligencia artificial sobre los derechos pueden acumularse progresivamente. En consecuencia, la reparación debe incluir, cuando resulte necesario, auditorías, modificación de criterios, actualización de datos, fortalecimiento de supervisión humana o suspensión temporal del sistema hasta corregir las causas que produjeron la vulneración.

La reparación debe considerar también la dimensión procedimental del daño. Fischman-Afori (2025) sostiene que las garantías de debido proceso pueden incorporarse desde el diseño de los sistemas de inteligencia artificial. Esta perspectiva permite comprender que una vulneración no siempre deriva exclusivamente del resultado final; también puede originarse en la falta de información, ausencia de audiencia, imposibilidad de presentar observaciones o inexistencia de una revisión humana adecuada. En estos supuestos, la reparación puede exigir repetir el procedimiento con garantías suficientes. Restituir derechos implica entonces asegurar que la nueva decisión sea adoptada mediante un proceso transparente, contradictorio, motivado y sometido a control efectivo.

Los mecanismos internacionales también respaldan la existencia de recursos efectivos. La Convención Americana sobre Derechos Humanos (1969), en su artículo 25, reconoce el derecho a un recurso sencillo, rápido y efectivo ante jueces o tribunales competentes frente a actos que vulneren derechos fundamentales. En materia de inteligencia artificial, el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 14, exige recursos accesibles y efectivos frente a vulneraciones vinculadas con sistemas de inteligencia artificial. Estos estándares refuerzan la obligación de evitar que la complejidad algorítmica se convierta en obstáculo para obtener reparación.

La reparación también exige identificar responsabilidades y asegurar seguimiento posterior. Una orden de corregir un sistema pierde efectividad si la administración no verifica

posteriormente su cumplimiento. Dragomir et al. (2026) relacionan responsabilidad institucional, derechos fundamentales y gobernanza de inteligencia artificial dentro de la administración pública. Esta perspectiva exige documentar medidas correctivas, asignar responsables y comprobar que los cambios implementados reduzcan efectivamente el riesgo. Cuando una vulneración revela fallas organizativas, la reparación puede requerir capacitación, nuevas reglas de supervisión, mejoras en contratación tecnológica o mecanismos de auditoría capaces de impedir que el mismo problema se reproduzca en otros procedimientos.

Los mecanismos de reparación y restitución deben concebirse, finalmente, como parte integral de la gobernanza pública de sistemas automatizados. Una administración responsable no solo previene riesgos, sino que dispone de procedimientos capaces de corregir decisiones, restituir derechos, compensar daños y modificar sistemas cuando se demuestra una vulneración. Los artículos 11, numeral 9, 75 y 92 de la Constitución de la República del Ecuador (2008), junto con el artículo 18 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), ofrecen fundamentos claros para estas medidas. La automatización solo puede considerarse legítima cuando existen remedios efectivos frente a sus posibles consecuencias lesivas.

5.8 Garantías institucionales para una automatización pública compatible con los derechos humanos

La compatibilidad entre automatización pública y derechos humanos depende de garantías institucionales que acompañen todo el ciclo de vida de los sistemas utilizados por la administración. No resulta suficiente incorporar tecnología eficiente si la institución carece de reglas para evaluar riesgos, documentar decisiones, supervisar resultados y responder frente a posibles vulneraciones. La Constitución de la República del Ecuador (2008), en su artículo 227, dispone que la administración pública constituye un servicio a la colectividad y se rige, entre otros, por los principios de eficacia, transparencia y evaluación. Estos principios obligan a integrar la innovación tecnológica dentro de estructuras institucionales orientadas al respeto efectivo de derechos.

Una primera garantía consiste en establecer una gobernanza clara de los sistemas algorítmicos. Esto requiere definir qué unidades autorizan su utilización, quién supervisa su funcionamiento, qué servidores pueden interpretar sus resultados y cuáles son los procedimientos para suspenderlos cuando aparezcan riesgos. Dragomir et al. (2026) vinculan la gobernanza de inteligencia artificial con responsabilidad, protección de derechos fundamentales y resiliencia

institucional. El Código Orgánico Administrativo (2017), en su artículo 14, establece además el principio de juridicidad. Por consiguiente, las responsabilidades tecnológicas deben integrarse a la estructura administrativa existente y no quedar dispersas entre proveedores, departamentos técnicos y funcionarios sin competencias claramente determinadas.

La evaluación preventiva constituye otra garantía institucional fundamental. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 42, exige evaluaciones de impacto cuando determinados tratamientos puedan generar alto riesgo para los derechos y libertades. En sistemas automatizados públicos, esta herramienta permite analizar anticipadamente posibles afectaciones relacionadas con privacidad, discriminación, errores de clasificación o decisiones difíciles de impugnar. Thomaidou y Limniotis (2025) destacan la utilidad de las evaluaciones de impacto para vincular protección de datos con derechos fundamentales. La evaluación debe efectuarse antes de implementar tecnologías de riesgo y actualizarse cuando cambien datos, finalidades, modelos o condiciones de funcionamiento.

La supervisión permanente constituye una garantía distinta de la evaluación inicial. Un sistema que funciona adecuadamente durante su implementación puede desarrollar errores, perder precisión o producir efectos diferenciados cuando cambian los datos o el contexto social. Vatamanu y Tofan (2025) advierten que la integración de inteligencia artificial en la administración pública genera desafíos y vulnerabilidades que requieren capacidad institucional sostenida. Por ello, las entidades deben establecer indicadores, auditorías periódicas, registros de incidentes y procedimientos de revisión. El control debe considerar tanto desempeño técnico como consecuencias jurídicas, porque una herramienta estadísticamente precisa puede producir resultados incompatibles con igualdad, proporcionalidad o debido proceso.

La capacidad humana de la institución constituye igualmente una garantía indispensable. Los servidores que utilizan sistemas automatizados deben comprender sus funciones, limitaciones y posibles errores para evitar una dependencia irreflexiva de las recomendaciones tecnológicas. Green (2022) advierte que la supervisión humana puede perder eficacia cuando se reduce a una formalidad, mientras que Alon-Barkat y Busuioc (2023) evidencian la influencia que el asesoramiento algorítmico puede ejercer sobre las decisiones de funcionarios. La capacitación debe incluir no solo conocimientos tecnológicos, sino también protección de datos, igualdad, motivación, transparencia y derechos humanos, asegurando que la responsabilidad decisoria continúe siendo jurídicamente identificable.

Tabla 18

Garantías institucionales para una automatización pública compatible con los derechos humanos

Garantía institucional	Contenido principal	Función preventiva	Fundamento o referente
Gobernanza algorítmica	Definición de competencias y responsables	Evitar responsabilidades difusas	Constitución, art. 227; COA, art. 14
Evaluación de impacto	Identificación previa de riesgos	Prevenir afectaciones de derechos	LOPDP, art. 42
Supervisión continua	Seguimiento, auditoría e indicadores	Detectar errores y efectos imprevistos	UNESCO (2021), párrs. 35–40
Capacitación institucional	Formación técnica, jurídica y ética	Reducir dependencia tecnológica	Reglamento (UE) 2024/1689, art. 14
Trazabilidad	Registro de datos, versiones y actuaciones	Facilitar control y responsabilidad	LOPDP, art. 20
Transparencia	Información sobre sistemas y decisiones	Permitir control ciudadano	Constitución, art. 18
Revisión y reclamación	Procedimientos accesibles de contradicción	Corregir decisiones lesivas	Constitución, arts. 75 y 76
Gestión de riesgos	Evaluación y mitigación permanente	Evitar vulneraciones sistemáticas	Consejo de Europa (2024), art. 16

Nota. Las garantías deben operar de manera articulada durante el diseño, implementación, funcionamiento, revisión y eventual retiro de los sistemas automatizados utilizados por instituciones públicas.

La trazabilidad institucional permite transformar estas garantías en mecanismos efectivos de rendición de cuentas. Una entidad debe conservar información sobre las versiones del sistema utilizadas, datos relevantes, resultados generados, intervenciones humanas y modificaciones realizadas durante su funcionamiento. Cheong (2024) destaca la estrecha relación entre transparencia y responsabilidad en sistemas de inteligencia artificial. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce garantías para conocer criterios de valoración, tipos y fuentes de datos empleados en determinadas decisiones automatizadas. Sin registros suficientes, posteriormente resulta difícil reconstruir una actuación, identificar errores, determinar responsabilidades o reparar adecuadamente una vulneración.

La protección institucional requiere además mecanismos accesibles de reclamación y revisión. La Constitución de la República del Ecuador (2008), en sus artículos 75 y 76, garantiza tutela efectiva y debido proceso, derechos que deben preservarse cuando una actuación

administrativa incorpora inteligencia artificial. Fischman-Afori (2025) sostiene que las garantías procedimentales pueden integrarse desde el diseño de los sistemas, evitando que la protección aparezca únicamente después del daño. Una institución compatible con este enfoque debe informar cómo cuestionar una decisión, permitir aportar observaciones, asegurar revisión humana y conservar procedimientos capaces de corregir tanto el resultado individual como las causas estructurales que lo produjeron.

Los estándares internacionales refuerzan la necesidad de institucionalizar estas salvaguardias. El Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (2024), en su artículo 16, exige mecanismos para identificar, evaluar, prevenir y mitigar riesgos e impactos sobre derechos. Como referencia comparada, el Reglamento (UE) 2024/1689 establece en su artículo 9 un sistema de gestión de riesgos para aplicaciones de alto riesgo y, en su artículo 27, evaluaciones de impacto sobre derechos fundamentales en determinados supuestos. Estas disposiciones muestran que la protección no debe depender de respuestas improvisadas, sino de estructuras permanentes de prevención, seguimiento y corrección.

Una automatización pública compatible con los derechos humanos requiere, finalmente, instituciones capaces de gobernar la tecnología y no limitarse a utilizarla. La Constitución de la República del Ecuador (2008), especialmente en sus artículos 18, 75, 76 y 227, ofrece fundamentos relacionados con transparencia, tutela, debido proceso y principios de la administración pública. Estos deben articularse con protección de datos, auditoría, gestión de riesgos, supervisión humana y mecanismos de reparación. La tecnología puede contribuir a mejorar la gestión estatal, pero su legitimidad dependerá de que existan capacidades institucionales suficientes para prevenir daños, explicar decisiones, atribuir responsabilidades y corregir oportunamente cualquier afectación de derechos.

Conclusión

La automatización de las decisiones públicas representa una de las transformaciones más relevantes de la administración contemporánea. La incorporación de inteligencia artificial, sistemas algorítmicos y herramientas automatizadas puede mejorar la capacidad institucional para procesar información, organizar procedimientos y responder con mayor rapidez a determinadas necesidades ciudadanas. Sin embargo, esta transformación no puede valorarse únicamente desde criterios de eficiencia o innovación. Cuando la tecnología interviene en actuaciones estatales capaces de afectar derechos, obligaciones o intereses legítimos, su utilización debe permanecer sometida al ordenamiento jurídico y a las garantías que limitan el ejercicio del poder público.

El análisis desarrollado demuestra que la automatización administrativa no constituye una realidad homogénea. Existen sistemas destinados únicamente a organizar información y otros capaces de clasificar personas, elaborar perfiles, establecer niveles de riesgo o formular recomendaciones que pueden condicionar significativamente una decisión. Esta diversidad obliga a evaluar cada tecnología según su finalidad, grado de autonomía, datos utilizados y consecuencias jurídicas. Cuanto mayor sea la incidencia del sistema sobre la situación de las personas, mayores deben ser las exigencias de supervisión, trazabilidad, explicación y control. La automatización no puede convertirse en una vía para trasladar potestades públicas a mecanismos tecnológicos carentes de suficiente vigilancia institucional.

La igualdad y la no discriminación constituyen límites fundamentales frente al uso de algoritmos en la administración pública. Los sistemas automatizados pueden reproducir desigualdades contenidas en datos históricos, utilizar variables indirectamente vinculadas con condiciones protegidas o generar errores distribuidos de manera desigual entre distintos grupos. Por ello, no resulta suficiente afirmar que una herramienta aplica las mismas reglas a todas las personas. Es necesario evaluar sus consecuencias concretas y determinar si produce exclusiones, cargas o diferencias injustificadas. Esta obligación adquiere especial relevancia cuando las decisiones afectan a grupos vulnerables o a personas que enfrentan mayores dificultades para cuestionar resultados automatizados.

La privacidad y la protección de datos personales constituyen igualmente condiciones estructurales para una automatización legítima. La creciente capacidad de integrar registros, construir perfiles y generar inferencias incrementa las posibilidades de conocer aspectos cada vez más amplios de la vida de las personas. La administración debe limitar el tratamiento a

información jurídicamente autorizada, pertinente y necesaria para finalidades determinadas. La disponibilidad tecnológica de los datos no equivale a libertad para utilizarlos. Además, los sistemas deben incorporar medidas de seguridad, calidad, minimización y proporcionalidad que reduzcan riesgos derivados de errores, accesos indebidos, reutilizaciones incompatibles o decisiones sustentadas en información desactualizada.

La transparencia y la explicabilidad aparecen como condiciones indispensables para evitar que la automatización produzca decisiones públicas incomprensibles. La ciudadanía debe poder identificar cuándo intervino un sistema automatizado, cuál fue su función, qué información relevante utilizó y cómo influyó en el resultado. La administración tampoco puede considerar suficiente la publicación de documentos técnicos que resulten inaccesibles para la mayoría de las personas. La información debe permitir comprender la decisión concreta. Explicar no significa necesariamente revelar cada detalle matemático del algoritmo, sino proporcionar razones suficientes para identificar criterios relevantes, detectar posibles errores y evaluar si la actuación se encuentra jurídicamente justificada.

El debido proceso conserva plena vigencia frente a cualquier modalidad de automatización pública. Las personas deben mantener posibilidades reales de conocer las actuaciones que las afectan, presentar observaciones, corregir información, cuestionar criterios y solicitar una revisión independiente del resultado automatizado. La intervención humana desempeña aquí una función esencial, siempre que sea sustantiva. La presencia formal de un funcionario no constituye una garantía cuando este carece de autonomía, información o capacidad para apartarse de la recomendación tecnológica. La supervisión efectiva exige servidores preparados para valorar las particularidades del caso y asumir responsabilidad por la decisión finalmente adoptada.

El derecho de impugnación y el control administrativo y judicial resultan indispensables para impedir que los resultados algorítmicos adquieran un carácter prácticamente irreversible. Las instituciones deben conservar registros que permitan reconstruir el proceso decisorio, identificar los datos utilizados, conocer la versión del sistema empleada y determinar quién intervino en cada etapa. Esta trazabilidad facilita auditorías, reclamaciones y revisiones posteriores. Cuando los mecanismos administrativos no sean suficientes, debe existir la posibilidad de acudir a instancias judiciales capaces de examinar la legalidad de la actuación. La complejidad tecnológica no puede convertirse en una barrera para ejercer tutela efectiva frente a decisiones públicas.

La determinación de responsabilidad constituye otro componente central de una gobernanza algorítmica compatible con los derechos humanos. La intervención de desarrolladores, proveedores tecnológicos, unidades administrativas y servidores públicos puede dificultar la identificación de responsabilidades, pero no debe generar espacios de irresponsabilidad. La institución que incorpora un sistema dentro del ejercicio de sus competencias continúa obligada a controlar su funcionamiento y responder por las decisiones adoptadas. La contratación de una herramienta externa tampoco permite trasladar completamente esta responsabilidad. Una administración responsable debe establecer previamente competencias, mecanismos de supervisión y procedimientos para identificar el origen de errores y adoptar medidas correctivas.

La reparación constituye la consecuencia necesaria cuando una decisión automatizada vulnera derechos. La respuesta no debe limitarse a reconocer la existencia del problema, sino que debe procurar restituir la situación afectada y evitar nuevas consecuencias. Dependiendo del caso, esto puede requerir rectificación de datos, eliminación de perfiles, repetición del procedimiento, modificación de criterios, suspensión del sistema, compensación o adopción de garantías de no repetición. Los daños algorítmicos también pueden presentar carácter estructural cuando un mismo error se reproduce entre numerosas personas. En esas situaciones, la reparación individual debe acompañarse de medidas dirigidas a corregir las causas tecnológicas e institucionales que originaron la afectación.

En definitiva, una administración pública tecnológicamente avanzada no debe medirse únicamente por la cantidad de procesos automatizados, sino por su capacidad para utilizar esas herramientas sin debilitar derechos. La automatización compatible con los derechos humanos requiere juridicidad, igualdad, protección de datos, transparencia, explicabilidad, supervisión humana, debido proceso, mecanismos de impugnación, responsabilidad y reparación. Estos elementos deben integrarse desde el diseño hasta la eventual retirada del sistema. La tecnología puede contribuir a una gestión pública más eficiente, pero su legitimidad dependerá de que permanezca bajo control humano e institucional y de que las personas continúen ocupando el centro de toda decisión pública.

Bibliografía

- Alon-Barkat, S., y Busuioc, M. (2023). Human–AI Interactions in Public Sector Decision Making: “Automation Bias” and “Selective Adherence” to Algorithmic Advice. *Journal of Public Administration Research and Theory*, 33(1), 153–169. <https://doi.org/10.1093/jopart/muac007>
- Alzoubi, Y., y Mishra, A. (2025). Differential Privacy and Artificial Intelligence: Potentials, Challenges, and Future Avenues. *EURASIP Journal on Information Security*, 2025, 18. <https://doi.org/10.1186/s13635-025-00203-9>
- Ameen, K., Towfiq, T., Mousa, K., y Pooyanmehr, M. (2026). Judicial Review of Algorithmic Administrative Systems: Legality, Evidence and Remedies in the Smart City State. *Frontiers in Artificial Intelligence*, 9, 1802986. <https://doi.org/10.3389/frai.2026.1802986>
- Arnesen, L. (2026). Comparing the Right to Information About Automated Decision-Making to the New Right to Explanation. *International Data Privacy Law*, 16(2), ipag008. <https://doi.org/10.1093/idpl/ipag008>
- Babšek, M., Ravšelj, D., Umek, L., y Aristovnik, A. (2025). Artificial Intelligence Adoption in Public Administration: An Overview of Top-Cited Articles and Practical Applications. *AI*, 6(3), 44. <https://doi.org/10.3390/ai6030044>
- Bayamlioğlu, E. (2022). The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the So-Called “Right to Explanation”. *Regulation & Governance*, 16(4), 1058–1078. <https://doi.org/10.1111/rego.12391>
- Binns, R., y Veale, M. (2021). Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law*, 11(4), 319–332. <https://doi.org/10.1093/idpl/ipab020>
- Chen, T., Gascó-Hernandez, M., y Esteve, M. (2024). The Adoption and Implementation of Artificial Intelligence Chatbots in Public Organizations: Evidence from U.S. State Governments. *The American Review of Public Administration*, 54(3), 255–270. <https://doi.org/10.1177/02750740231200522>
- Cheong, B. (2024). Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making. *Frontiers in Human Dynamics*, 6, 1421273. <https://doi.org/10.3389/fhumd.2024.1421273>

- Christodoulou, P., y Limniotis, K. (2024). Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges. *Network*, 4(1), 91–113. <https://doi.org/10.3390/network4010005>
- Código Orgánico Administrativo*. (2017). Registro Oficial, Segundo Suplemento No. 31, 7 de julio de 2017: https://www.defensa.gob.ec/wp-content/uploads/downloads/2023/03/COA_feb_2023.pdf
- Consejo de Europa*. (2024). Convenio Marco del Consejo de Europa sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho (CETS No. 225): <https://www.boe.es/doue/2026/1081/L00001-00013.pdf>
- Constitución de la República del Ecuador*. (2008). Registro Oficial No. 449, 20 de octubre de 2008: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf
- Convención Americana sobre Derechos Humanos (Pacto de San José)*. (1969). Organización de los Estados Americanos: <https://www.oas.org/es/cidh/mandato/documentos-basicos/convencion-americana-derechos-humanos.pdf>
- Custers, B., y Heijne, A.-S. (2022). The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice. *Computer Law & Security Review*, 46, 105727. <https://doi.org/10.1016/j.clsr.2022.105727>
- Declaración Universal de Derechos Humanos*. (1948). <https://www.un.org/es/about-us/universal-declaration-of-human-rights>
- Dexe, J., Franke, U., Söderlund, K., Berkel, N., Jensen, R., Lepinkäinen, N., y Vaiste, J. (2022). Explaining Automated Decision-Making: A Multinational Study of the GDPR Right to Meaningful Information. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 47(3), 669–697. <https://doi.org/10.1057/s41288-022-00271-9>
- Dragomir, A., Bulea, I., y Tarnu, L. (2026). Human-Centric AI Governance in the European Union: Accountability, Fundamental Rights, and Institutional Resilience in Public Administration. *Frontiers in Political Science*, 8, 1928481. <https://doi.org/10.3389/fpos.2026.1928481>
- Fischman-Afori, O. (2025). Due Process by Design: Enhancing Fairness and Trust in AI Decision-Making. *Social Sciences & Humanities Open*, 12, 102178. <https://doi.org/10.1016/j.ssaho.2025.102178>

- Freitas, J. (2026). The Challenges of AI Regulation: Data Protection, Civil Rights, and Landmark Cases. *Frontiers in Political Science*, 8, 1626848. <https://doi.org/10.3389/fpos.2026.1626848>
- Grant, D., Behrends, J., y Basl, J. (2025). What We Owe to Decision-Subjects: Beyond Transparency and Explanation in Automated Decision-Making. *Philosophical Studies*, 182, 55–85. <https://doi.org/10.1007/s11098-023-02013-6>
- Green, B. (2022). The Flaws of Policies Requiring Human Oversight of Government Algorithms. *Computer Law & Security Review*, 45, 105681. <https://doi.org/10.1016/j.clsr.2022.105681>
- Grimmelikhuijsen, S. (2023). Explaining Why the Computer Says No: Algorithmic Transparency Affects the Perceived Trustworthiness of Automated Decision-Making. *Public Administration Review*, 83(2), 241–262. <https://doi.org/10.1111/puar.13483>
- Grimmelikhuijsen, S., y Meijer, A. (2022). Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response. *Perspectives on Public Management and Governance*, 5(3), 232–242. <https://doi.org/10.1093/ppmgov/gvac008>
- He, J., y Zhang, Z. (2025). Algorithm Power and Legal Boundaries: Rights Conflicts and Governance Responses in the Era of Artificial Intelligence. *Laws*, 14(4), 54. <https://doi.org/10.3390/laws14040054>
- Lendvai, G., y Gosztonyi, G. (2025). Algorithmic Bias as a Core Legal Dilemma in the Age of Artificial Intelligence: Conceptual Basis and the Current State of Regulation. *Laws*, 14(3), 41. <https://doi.org/10.3390/laws14030041>
- Ley del Sistema Nacional de Registro de Datos Públicos*. (2010). Registro Oficial, Suplemento No. 162, 31 de marzo de 2010: <https://www.gob.ec/sites/default/files/regulations/2018-10/LEY%20SINARDAP.pdf>
- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. (2009). Registro Oficial, Segundo Suplemento No. 52, 22 de octubre de 2009: <https://biblioteca.defensoria.gob.ec/bitstream/37000/3823/3/Ley%20Org%20de%20Garant%20Jurisdiccionales%20y%20Control%20Constitucional.%20reforma.pdf>
- Ley Orgánica de Protección de Datos Personales*. (2021). Registro Oficial, Quinto Suplemento No. 459, 26 de mayo de 2021: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/LOPD-LEXIS.pdf>

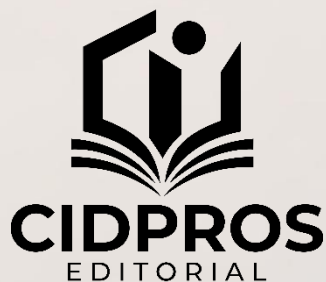
- Ley Orgánica de Transparencia y Acceso a la Información Pública*. (2023). Registro Oficial, Segundo Suplemento No. 245, 7 de febrero de 2023: <https://www.gob.ec/sites/default/files/regulations/2020-06/LOTAIP.pdf>
- Lütz, F. (2022). Gender Equality and Artificial Intelligence in Europe: Addressing Direct and Indirect Impacts of Algorithms on Gender-Based Discrimination. *ERA Forum*, 23, 33–52. <https://doi.org/10.1007/s12027-022-00709-6>
- Medrano-Sánchez, E., Ruiz-Ramírez, E., y Ayllon, M. (2026). Between Innovation and Risk: Artificial Intelligence and Data Protection in Digital Mexico. *Frontiers in Artificial Intelligence*, 9, 1716108. <https://doi.org/10.3389/frai.2026.1716108>
- Metikos, L. (2024). Explaining and Contesting Judicial Profiling Systems. *Technology and Regulation*, 2024, 188–208. <https://doi.org/10.71265/azacz070>
- Murdoch, B. (2021). Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era. *BMC Medical Ethics*, 22, 122. <https://doi.org/10.1186/s12910-021-00687-3>
- Neumann, O., Guirguis, K., y Steiner, R. (2024). Exploring Artificial Intelligence Adoption in Public Organizations: A Comparative Case Study. *Public Management Review*, 26(1), 114–141. <https://doi.org/10.1080/14719037.2022.2048685>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2021). Recomendación sobre la ética de la inteligencia artificial. UNESCO: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Pacto Internacional de Derechos Civiles y Políticos*. (1966). <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Papadimitriou, E. (2023). The Right to Explanation in the Processing of Personal Data with the Use of AI Systems. *International Journal of Law in Changing World*, 2(2), 43–55. <https://doi.org/10.54934/ijlcw.v2i2.53>
- Parlamento Europeo & Consejo de la Unión Europea*. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Peters, U. (2023). Explainable AI Lacks Regulative Reasons: Why AI and Human Decision-Making Are Not Equally Opaque. *AI and Ethics*, 3, 963–974. <https://doi.org/10.1007/s43681-022-00217-w>

- Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904)*. (2023). Oficial, Tercer Suplemento No. 435, 13 de noviembre de 2023: https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf
- Sanchez-Graells, A. (2024). Resh(AI)ping Good Administration: Addressing the Mass Effects of Public Sector Digitalisation. *Laws*, 13(1), 9. <https://doi.org/10.3390/laws13010009>
- Savveli, I., Rigou, M., y Balaskas, S. (2025). From E-Government to AI E-Government: A Systematic Review of Citizen Attitudes. *Informatics*, 12(3), 98. <https://doi.org/10.3390/informatics12030098>
- Teo, S. (2025). Artificial Intelligence and Its ‘Slow Violence’ to Human Rights. *AI and Ethics*, 5, 2265–2280. <https://doi.org/10.1007/s43681-024-00547-x>
- Thomaidou, A., y Limniotis, K. (2025). Navigating Through Human Rights in AI: Exploring the Interplay Between GDPR and Fundamental Rights Impact Assessment. *Journal of Cybersecurity and Privacy*, 5(1), 7. <https://doi.org/10.3390/jcp5010007>
- van Noordt, C., y Misuraca, G. (2022). Exploratory Insights on Artificial Intelligence for Government in Europe. *Social Science Computer Review*, 40(2), 426–444. <https://doi.org/10.1177/0894439320980449>
- Vatamanu, A., y Tofan, M. (2025). Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. *Administrative Sciences*, 15(4), 149. <https://doi.org/10.3390/admsci15040149>
- Voloch, N., y Hirschprung, R. (2026). Both Ends of Artificial Intelligence Impacting Privacy: A Review of Violation and Protection. *Frontiers in Artificial Intelligence*, 9, 1686454. <https://doi.org/10.3389/frai.2026.1686454>
- Wang, X., Wu, Y., Ji, X., y Fu, H. (2024). Algorithmic Discrimination: Examining Its Types and Regulatory Measures with Emphasis on US Legal Practices. *Frontiers in Artificial Intelligence*, 7, 1320277. <https://doi.org/10.3389/frai.2024.1320277>
- Warthon, M. (2024). Restricting Access to AI Decision-Making in the Public Interest: The Justificatory Role of Proportionality and Its Balancing Factors. *Internet Policy Review*, 13(3). <https://doi.org/10.14763/2024.3.1801>
- Yigitcanlar, T., David, A., Li, W., Fookes, C., Bibri, S., y Ye, X. (2024). Unlocking Artificial Intelligence Adoption in Local Governments: Best Practice Lessons from Real-World Implementations. *Smart Cities*, 7(4), 1576–1625. <https://doi.org/10.3390/smartcities7040064>

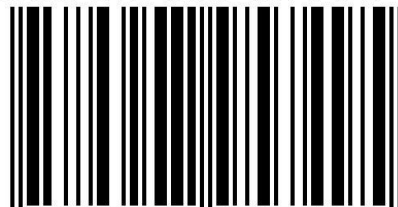
- Yoon, H., Belkhouja, M., y Dau, L. (2025). Privacy Protection Laws, National Culture, and Artificial Intelligence Innovation Around the World. *Journal of International Business Studies*, 56, 853–873. <https://doi.org/10.1057/s41267-025-00790-2>
- Zuiderwijk, A., Chen, Y.-C., y Salem, F. (2021). Implications of the Use of Artificial Intelligence in Public Governance: A Systematic Literature Review and a Research Agenda. *Government Information Quarterly*, 38(3), 101577. <https://doi.org/10.1016/j.giq.2021.101577>

DERECHOS HUMANOS

frente a la automatización
de las decisiones públicas



ISBN: 978-9907-9574-9-5



9 789907 957495