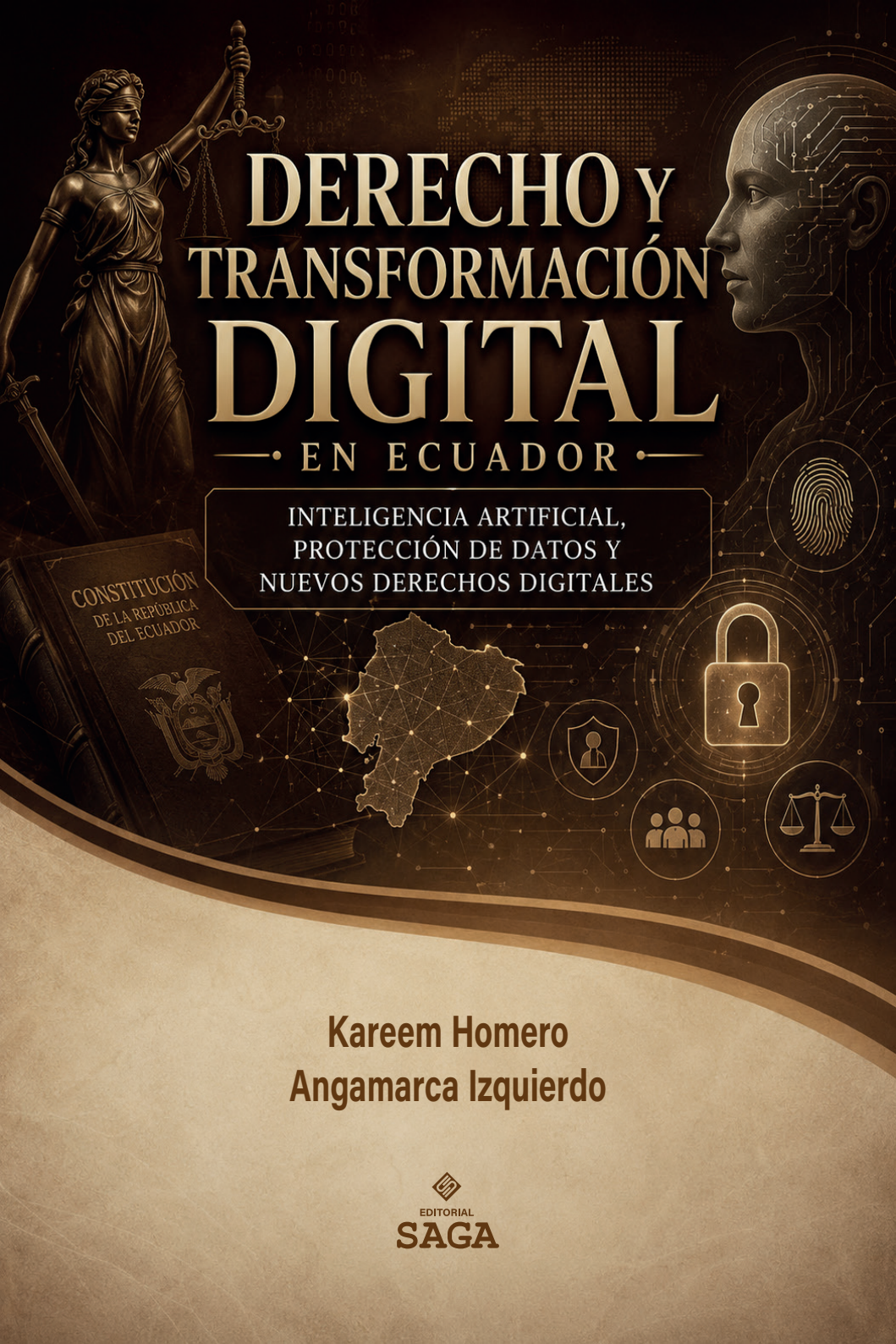




DERECHO Y TRANSFORMACIÓN DIGITAL

— • EN ECUADOR • —

INTELIGENCIA ARTIFICIAL,
PROTECCIÓN DE DATOS Y
NUEVOS DERECHOS DIGITALES

Kareem Homero
Angamarca Izquierdo

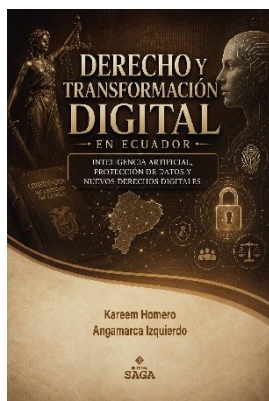

EDITORIAL
SAGA

Derecho y Transformación Digital en Ecuador

**Inteligencia Artificial, Protección
de Datos y Nuevos Derechos
Digitales**



Autor:
Kareem Homero Angamarca Izquierdo



Datos bibliográficos

ISBN:	978-9907-803-63-1
Título del libro:	Derecho y Transformación Digital en Ecuador Inteligencia Artificial, Protección de Datos y Nuevos Derechos Digitales
Autores:	Angamarca Izquierdo, Kareem Homero
Editorial:	SAGA
Materia:	370 - Educación
Público objetivo:	Profesional / académico
Publicado:	2026-08-11
Número de edición:	1
Tamaño:	5Mb
Soporte:	Libro digital descargable
Formato:	Pdf (.pdf)
Idioma:	Español
DOI:	https://doi.org/10.63415/saga.2026.117

Hecho en Ecuador / Made in Ecuador

Autores

Kareem Homero Angamarca Izquierdo

Universidad César Vallejo

✉ ab.homeroangamarca@hotmail.com

id <https://orcid.org/0000-0002-7676-8089>

Quevedo, Ecuador

Kareem Homero Angamarca Izquierdo es profesional del ámbito jurídico y de la gestión pública, vinculado académicamente a la Universidad César Vallejo. Es Maestro en Gestión Pública por esta institución y Abogado por la Universidad Técnica Particular de Loja. Su formación articula conocimientos jurídicos con herramientas de administración y gestión pública, configurando un perfil orientado al análisis de las relaciones entre el Estado, el ordenamiento jurídico y los derechos ciudadanos.

Su actividad investigativa se concentra en problemáticas jurídicas y sociales relacionadas con la actuación estatal, los derechos fundamentales, la propiedad y la gestión de los espacios públicos. Entre sus publicaciones se encuentran *Uso arbitrario de bienes privados por el Estado como forma de confiscación* y *Apropiación de espacios privados para uso público: análisis empírico en Los Ríos, Ecuador*. También registra participación en investigaciones relacionadas con los desafíos constitucionales derivados de la inteligencia artificial y la protección de los derechos fundamentales, ampliando su campo de análisis hacia las implicaciones jurídicas de las tecnologías emergentes.

Su trayectoria académica refleja interés por vincular el derecho, la gestión pública y la investigación científica, aportando al análisis crítico de las actuaciones estatales y de los desafíos jurídicos contemporáneos desde una perspectiva orientada a la protección de derechos.



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

Derecho y Transformación Digital en Ecuador: Inteligencia Artificial, Protección de Datos y Nuevos Derechos Digitales examina las transformaciones que las tecnologías digitales producen en el ordenamiento jurídico ecuatoriano, con especial atención a la inteligencia artificial, la protección de datos personales y la configuración contemporánea de los derechos digitales. La obra articula una lectura constitucional, normativa e institucional destinada a comprender las relaciones entre innovación tecnológica, dignidad humana, autonomía, privacidad y responsabilidad jurídica. Desde una perspectiva académica e interdisciplinaria, analiza la incidencia de los sistemas algorítmicos en las decisiones públicas y privadas, el tratamiento automatizado de información, los datos biométricos, la identidad digital, la discriminación algorítmica y la circulación transfronteriza de datos. Examina también la responsabilidad derivada de sistemas inteligentes, la autoría de contenidos sintéticos, los deepfakes, la desconexión digital, los neuroderechos y la tutela de la autonomía cognitiva. El estudio incorpora mecanismos regulatorios vinculados con auditorías algorítmicas, trazabilidad, evaluación de impacto, certificación tecnológica y espacios controlados de experimentación normativa. Bajo una perspectiva centrada en la persona, el libro plantea criterios para fortalecer la regulación ecuatoriana mediante garantías capaces de conciliar innovación, seguridad jurídica, transparencia y protección efectiva de derechos ante una sociedad progresivamente mediada por tecnologías digitales.

Palabras clave: inteligencia artificial, protección de datos, derechos humanos, derecho a la privacidad, tecnología de la información

Synopsis

Law and Digital Transformation in Ecuador: Artificial Intelligence, Data Protection and New Digital Rights examines the transformations that digital technologies produce within Ecuador's legal system, with particular attention to artificial intelligence, personal data protection, and the contemporary configuration of digital rights. The book develops a constitutional, regulatory, and institutional perspective aimed at understanding the relationships among technological innovation, human dignity, autonomy, privacy, and legal liability. From an academic and interdisciplinary perspective, it analyzes the influence of algorithmic systems on public and private decision-making, automated information processing, biometric data, digital identity, algorithmic discrimination, and cross-border data flows. It also examines liability arising from intelligent systems, authorship of synthetic content, deepfakes, the right to disconnect, neurorights, and the legal protection of cognitive autonomy. The study addresses regulatory mechanisms associated with algorithmic audits, traceability, impact assessments, technological certification, and controlled environments for regulatory experimentation. Adopting a human-centered perspective, the book develops criteria for strengthening Ecuadorian regulation through legal safeguards capable of reconciling innovation, legal certainty, transparency, and the effective protection of rights within a society increasingly mediated by digital technologies.

Keywords: artificial intelligence, data protection, human rights, right to privacy, information technology

Índice General

Sinopsis.....	v
Índice General	7
Introducción	11
Capítulo 1: Constitucionalismo digital y reconfiguración del orden jurídico ecuatoriano	15
1.1. La transformación digital como fenómeno de mutación del sistema jurídico ecuatoriano	19
1.2. Constitución, dignidad humana y autodeterminación en entornos digitales.....	22
1.3. Eficacia horizontal de los derechos constitucionales frente al poder tecnológico privado	26
1.4. Identidad digital, personalidad jurídica y construcción del sujeto en el ecosistema algorítmico	29
1.5. Ciudadanía digital y nuevas formas de participación, interacción y ejercicio democrático.....	33
1.6. Jurisdicción, territorialidad y soberanía estatal ante infraestructuras digitales transnacionales	36
Capítulo 2: Inteligencia artificial, decisión algorítmica y responsabilidad jurídica	41
2.1. Inteligencia artificial y capacidad regulatoria del ordenamiento jurídico ecuatoriano	45
2.2. Decisiones automatizadas, explicabilidad algorítmica y garantías del debido proceso	48
2.3. Sesgos algorítmicos, discriminación digital e igualdad constitucional.....	52
2.4. Responsabilidad civil, administrativa y penal por daños vinculados con sistemas de inteligencia artificial	55

2.5. Inteligencia artificial generativa, autoría y titularidad de contenidos sintéticos	59
2.6. Inteligencia artificial en la función pública: automatización administrativa, motivación y control judicial.....	62
Capítulo 3: Protección de datos personales y gobernanza jurídica de la información	69
3.1. La protección de datos personales como derecho autónomo en el sistema jurídico ecuatoriano.....	73
3.2. Consentimiento digital, bases de legitimación y límites jurídicos al tratamiento masivo de información.....	76
3.3. Perfilamiento, inferencias algorítmicas y tratamiento automatizado de datos personales	80
3.4. Datos biométricos, reconocimiento facial y vigilancia tecnológica	83
3.5. Transferencias internacionales de datos, servicios en la nube y soberanía informacional	87
3.6. Responsabilidad proactiva, evaluación de impacto y cumplimiento regulatorio basado en riesgos.....	90
Capítulo 4: Nuevos derechos digitales y tutela jurídica de la persona conectada	95
4.1. Configuración jurídica de los derechos digitales en el constitucionalismo contemporáneo	99
4.2. Derecho a la identidad digital y protección frente a la suplantación mediante inteligencia artificial.....	102
4.3. Derecho a la desconexión digital y límites jurídicos a la disponibilidad permanente	106
4.4. Derecho al olvido, memoria digital y permanencia de la información en internet	109
4.5. Neuroderechos, datos neuronales y protección jurídica de la autonomía cognitiva	113

4.6. Integridad informacional frente a deepfakes, clonación de voz y contenidos sintéticos hiperrealistas	116
Capítulo 5: Regulación tecnológica y construcción del Derecho Digital ecuatoriano.....	123
5.1. Hacia un modelo ecuatoriano de gobernanza jurídica de la inteligencia artificial.....	127
5.2. Regulación basada en niveles de riesgo y obligaciones diferenciadas para sistemas algorítmicos	130
5.3. Auditoría algorítmica, trazabilidad y certificación jurídica de sistemas de inteligencia artificial.....	134
5.4. Sandbox regulatorio como instrumento de experimentación jurídica para tecnologías de alto impacto	137
5.5. Coordinación entre autoridades de protección de datos, órganos judiciales y entidades de regulación tecnológica.....	141
5.6. Agenda legislativa para un estatuto ecuatoriano de derechos digitales e inteligencia artificial.....	144
Conclusiones	149
Referencias Bibliográficas.....	153
Advertencia jurídica	156

Introducción

La transformación digital ha dejado de ser un fenómeno periférico para convertirse en una fuerza que modifica las categorías mediante las cuales el Derecho comprende el poder, la autonomía y la protección de la persona. La expansión de sistemas algorítmicos, plataformas digitales e inteligencia artificial altera relaciones sociales e institucionales antes reguladas desde presupuestos predominantemente analógicos. Avbelj (2024) advierte que la sociedad gobernada crecientemente por algoritmos exige reconsiderar categorías constitucionales asentadas, debido a que la tecnología interviene cada vez con mayor intensidad en la organización y ejercicio del poder.

En Ecuador, esta transformación adquiere una dimensión jurídica particular. La Constitución de 2008 reconoce garantías relacionadas con la dignidad, intimidad, igualdad, identidad, libre desarrollo de la personalidad y protección de datos, mientras que la legislación posterior ha incorporado instrumentos orientados hacia la digitalización institucional y la tutela de la información personal. Zhao (2025) vincula la dignidad humana con la autonomía dentro de la gobernanza algorítmica, relación que permite comprender por qué la innovación tecnológica requiere examinarse desde los derechos fundamentales y no exclusivamente desde criterios de eficiencia.

La consolidación de entornos digitales también ha desplazado parte del poder hacia actores privados capaces de recopilar información, perfilar individuos e intervenir algorítmicamente en decisiones relevantes. Este cambio modifica las relaciones tradicionales entre ciudadanía, Estado y mercado. Frosio (2023) demuestra que la protección efectiva de los derechos fundamentales frente a las plataformas digitales requiere considerar las responsabilidades derivadas del poder tecnológico

privado. A ello se añade la fragmentación de la identidad personal en múltiples representaciones digitales que, como señalan Vardanyan, Hamulák y Kocharyan (2024), compromete la integridad y la autodeterminación informativa.

El estudio de estas transformaciones encuentra una justificación académica en la necesidad de integrar debates que con frecuencia aparecen examinados de manera separada. Inteligencia artificial, protección de datos y derechos digitales pertenecen a una misma reorganización jurídica de las relaciones entre tecnología y persona. Zaidan e Ibrahim (2024) muestran que la gobernanza de la inteligencia artificial se desarrolla dentro de un panorama regulatorio dinámico y multinivel. Por su parte, Mühlhoff (2024) evidencia que las inferencias y predicciones algorítmicas amplían las implicaciones de la protección de datos más allá de una concepción estrictamente individual.

Desde esta perspectiva, el libro tiene como objetivo general analizar las transformaciones producidas por las tecnologías digitales en el ordenamiento jurídico ecuatoriano, identificando garantías, tensiones regulatorias y criterios para una respuesta jurídica centrada en la persona. Se pretende, además, examinar la incidencia de la inteligencia artificial en las decisiones públicas y privadas, estudiar la gobernanza de los datos personales y sistematizar derechos vinculados con identidad, desconexión, memoria digital y autonomía cognitiva. Pangrazio y Sefton-Green (2021) permiten situar esta discusión al diferenciar derechos digitales, ciudadanía digital y alfabetización digital.

La investigación se articula alrededor de varias preguntas relacionadas entre sí: ¿en qué medida las categorías constitucionales ecuatorianas ofrecen respuestas adecuadas ante el poder algorítmico?, ¿qué garantías deben acompañar las decisiones automatizadas?, ¿qué límites jurídicos requiere el tratamiento intensivo de información personal?, ¿qué derechos necesitan una formulación específica frente a nuevas capacidades tecnológicas?

Estas interrogantes adquieren especial relevancia ante fenómenos como la discriminación algorítmica. Kelly-Lyth (2023), al estudiar sus manifestaciones en el ámbito laboral, evidencia que los sistemas automatizados pueden reproducir diferencias de trato con consecuencias jurídicas materiales.

El primer capítulo aborda el constitucionalismo digital y la reconfiguración del orden jurídico ecuatoriano. Su recorrido parte de la transformación digital como fenómeno de mutación jurídica y avanza hacia la dignidad, la autodeterminación, la eficacia horizontal de los derechos, la identidad y la ciudadanía digital, hasta alcanzar los problemas de jurisdicción y soberanía frente a infraestructuras transnacionales. Fahey (2023) relaciona soberanía digital, protección de datos y localización de información, mientras Gonzalez-Mohino et al. (2023) destacan el papel de las herramientas digitales en nuevas modalidades de participación ciudadana.

El segundo y el tercer capítulo concentran el análisis en la inteligencia artificial y la gobernanza jurídica de la información. El segundo examina decisiones automatizadas, explicabilidad, discriminación, responsabilidad, autoría de contenidos sintéticos y automatización administrativa. Rudolf y Kovač (2024) vinculan directamente la decisión automatizada con garantías administrativas y protección de datos. El tercero estudia consentimiento, perfilamiento, biometría, transferencias internacionales y responsabilidad proactiva. Santos et al. (2021) muestran que incluso la gestión del consentimiento digital plantea interrogantes acerca de responsabilidades y legitimidad del tratamiento informacional.

El cuarto capítulo dirige la atención hacia la persona conectada y los derechos que adquieren nueva expresión frente a tecnologías capaces de registrar, reproducir o intervenir aspectos de su identidad. Se examinan identidad digital, suplantación mediante inteligencia artificial, desconexión laboral, derecho al

olvido, neuroderechos e integridad informacional frente a deepfakes y contenidos sintéticos. Kiriak (2021) analiza las tensiones jurídicas asociadas con la permanencia de información en internet, mientras Moreira (2026) estudia las distintas vías regulatorias desarrolladas alrededor de los neuroderechos y la protección de la autonomía cognitiva.

El quinto capítulo proyecta el análisis hacia la construcción de un Derecho Digital ecuatoriano capaz de responder de manera sistemática a estas transformaciones. Se estudian gobernanza de inteligencia artificial, regulación basada en riesgos, auditoría algorítmica, trazabilidad, certificación, sandboxes regulatorios y coordinación institucional, para formular una agenda legislativa orientada a los derechos digitales. Sourdin (2025) aporta una perspectiva comparada sobre modelos de gobernanza, mientras Español (2025) concibe los espacios controlados de experimentación como mecanismos de aprendizaje regulatorio. El libro busca, en consecuencia, contribuir a una arquitectura jurídica ecuatoriana que concilie innovación, seguridad jurídica, transparencia, dignidad y protección efectiva de derechos.

Capítulo 1:

Constitucionalismo digital y reconfiguración del orden jurídico ecuatoriano

La transformación digital ha dejado de ocupar una posición periférica en el pensamiento jurídico. Hoy interviene en la manera de ejercer derechos, construir identidad, participar políticamente y relacionarse con instituciones públicas y actores privados. Avbelj (2024) advierte que la sociedad algorítmica obliga a reconsiderar categorías centrales del constitucionalismo contemporáneo. Para Ecuador, esta transformación plantea una cuestión de fondo: determinar hasta qué punto el orden constitucional puede gobernar relaciones humanas crecientemente mediadas por datos, algoritmos e infraestructuras digitales.

El punto de partida permanece en la persona. La tecnología adquiere relevancia constitucional cuando incide sobre libertad, autonomía, intimidad o posibilidades reales de decidir acerca de la propia existencia. Zhao (2025) vincula la dignidad humana con una gobernanza algorítmica orientada a preservar autonomía y agencia individual. Bajo esta perspectiva, los entornos digitales no constituyen espacios ajenos a la Constitución. Son escenarios donde antiguas garantías encuentran nuevas formas de ejercicio y donde el poder tecnológico requiere límites jurídicos reconocibles.

Esa presencia constitucional adquiere especial importancia frente al crecimiento de actores tecnológicos privados. Plataformas y empresas pueden organizar conversaciones públicas, procesar enormes cantidades de información y establecer condiciones capaces de afectar derechos. Frosio (2023) sostiene que la responsabilidad de las plataformas digitales debe construirse tomando seriamente los derechos fundamentales implicados. La cuestión resulta particularmente relevante para Ecuador, donde la eficacia horizontal permite comprender que determinadas relaciones entre particulares también pueden alcanzar una intensidad susceptible de tutela constitucional efectiva.

La identidad ofrece otra entrada al problema. Cada interacción digital deja datos que pueden autenticar, clasificar, describir e incluso anticipar comportamientos individuales.

Vardanyan et al. (2024) explican que la fragmentación de las identidades digitales mantiene estrechos vínculos con integridad personal y autodeterminación informativa. La persona aparece entonces representada mediante múltiples versiones construidas por sistemas tecnológicos. El derecho necesita preservar la distancia entre esas representaciones parciales y una personalidad jurídica que nunca puede reducirse enteramente a perfiles computacionales.

Figura 1
Ejes del constitucionalismo digital ecuatoriano



También cambia la experiencia de ciudadanía. La participación democrática transcurre ahora entre instituciones tradicionales y espacios digitales donde información, opiniones y movilizaciones circulan con enorme velocidad. Gonzalez-Mohino et al. (2023) relacionan las herramientas digitales con el fortalecimiento del pensamiento crítico y la participación ciudadana. Sin embargo, ampliar canales tecnológicos no garantiza por sí mismo una democracia más intensa. Acceso, alfabetización, deliberación reflexiva e igualdad constituyen condiciones

necesarias para convertir conectividad en auténtica capacidad de intervención pública.

La dimensión territorial agrega una tensión diferente. Los datos atraviesan fronteras mientras las personas permanecen sujetas a ordenamientos nacionales que deben garantizar sus derechos. Fahey (2023) examina la soberanía digital desde las relaciones entre protección jurídica, circulación internacional y localización de información. Para Ecuador, esta discusión alcanza jurisdicción y capacidad regulatoria. Una infraestructura situada en otro país puede producir efectos jurídicos internos, obligando a reconsiderar las conexiones tradicionales entre territorio, autoridad estatal y aplicación efectiva del derecho.

Estas transformaciones no ocurren de manera independiente. Identidad, autonomía, participación, poder privado y soberanía forman partes de una misma reorganización jurídica producida por la digitalización. Avbelj (2024) sitúa este fenómeno dentro de una revisión más amplia del constitucionalismo ante sociedades gobernadas crecientemente mediante procesos algorítmicos. La pregunta deja de concentrarse en adaptar normas aisladas a nuevas tecnologías. Interesa comprender qué ocurre con las categorías jurídicas cuando las condiciones materiales bajo las cuales fueron concebidas empiezan a modificarse profundamente.

El ordenamiento ecuatoriano posee herramientas relevantes para afrontar este proceso. La Constitución ofrece derechos y garantías capaces de proyectarse sobre relaciones digitales, mientras la legislación sobre protección de datos y transformación digital desarrolla respuestas específicas. Con todo, la norma escrita necesita dialogar permanentemente con transformaciones tecnológicas aceleradas. Zhao (2025) recuerda que una gobernanza algorítmica compatible con valores humanos requiere mantener la dignidad dentro de su estructura decisoria. Esa exigencia atraviesa necesariamente cualquier lectura constitucional de la digitalización.

Hay, además, una cuestión relacionada con la distribución del poder. Quien controla datos, infraestructuras o mecanismos de clasificación puede influir sobre oportunidades, información y decisiones que afectan la vida cotidiana. Frosio (2023) permite advertir que los derechos fundamentales constituyen parámetros relevantes para ordenar responsabilidades dentro de ecosistemas digitales privados. Vardanyan et al. (2024), desde otra perspectiva, muestran que esa influencia alcanza incluso la representación informacional del individuo. El constitucionalismo digital debe reconocer estas nuevas capacidades de intervención.

Este capítulo aborda, por tanto, una reconfiguración del orden jurídico ecuatoriano que atraviesa instituciones y categorías fundamentales. Desde la transformación digital hasta la soberanía frente a infraestructuras transnacionales, el hilo conductor permanece en la capacidad del derecho constitucional para preservar libertad, dignidad y participación. Gonzalez-Mohino et al. (2023) y Fahey (2023) permiten observar dimensiones ciudadanas y territoriales de este cambio. El constitucionalismo digital aparece, en consecuencia, como respuesta jurídica a una sociedad profundamente mediada por tecnología.

1.1. La transformación digital como fenómeno de mutación del sistema jurídico ecuatoriano

La transformación digital modifica la arquitectura del derecho ecuatoriano porque desplaza prácticas, lenguajes y centros tradicionales de decisión hacia entornos mediados por datos, plataformas y automatización. No se trata de incorporar herramientas a instituciones intactas, sino de advertir una mutación jurídica progresiva. Avbelj (2024) sostiene que la sociedad algorítmica tensiona categorías constitucionales heredadas y exige revisar sus fundamentos. En Ecuador, esta lectura permite entender la tecnología desde una dimensión constitucional, institucional y democrática ecuatoriana contemporánea.

La Constitución ecuatoriana ofrece un punto de partida normativo para comprender esa mutación. Los derechos a la comunicación, al acceso a información y al empleo de tecnologías de información proyectan garantías concebidas antes del actual despliegue algorítmico hacia relaciones digitales cada vez más densas (Constitución de la República del Ecuador, 2008, arts. 16 y 18). La norma constitucional adquiere, entonces, una función expansiva: sus principios deben gobernar espacios técnicos donde también circula poder jurídico efectivo.

La Ley Orgánica para la Transformación Digital y Audiovisual convierte este tránsito en política jurídica explícita. Su artículo 1 promueve la simplificación y adopción de medios y tecnologías digitales en servicios públicos, trámites administrativos, actuaciones judiciales y actividades privadas (Ley Orgánica para la Transformación Digital y Audiovisual, 2023). La transformación deja de aparecer vinculada únicamente con eficiencia técnica. Pasa a incidir en procedimientos, competencias institucionales y formas de relación entre ciudadanía, administración y mercado ecuatoriano.

Este desplazamiento obliga a reconsiderar la idea clásica de autoridad. En una administración digitalizada, decisiones relevantes pueden depender de arquitecturas informáticas, reglas automatizadas y sistemas cuya operación resulta poco visible para el ciudadano. Avbelj (2024) advierte que la expansión de la inteligencia artificial produce una brecha epistemológica para el constitucionalismo contemporáneo. La cuestión ecuatoriana rebasa, por ello, la mera modernización estatal: interesa determinar quién decide, mediante qué criterios y bajo cuáles garantías constitucionales efectivas reales.

El Reglamento General profundiza esta orientación al ordenar procedimientos para aplicar eficientemente la ley y articular planes, programas y proyectos de transformación digital (Reglamento General a la Ley Orgánica para la Transformación

Digital y Audiovisual, 2023, arts. 1-2). Tal diseño revela una característica importante: la digitalización jurídica requiere conducción institucional. La tecnología no actúa en vacío; queda incorporada a competencias, políticas públicas, presupuestos y mecanismos administrativos que deben permanecer sometidos al principio de juridicidad democrático.

La mutación también alcanza la experiencia cotidiana de los derechos. Una garantía constitucional puede conservar idéntica redacción y, pese a ello, cambiar profundamente cuando su ejercicio depende de identificación digital, interoperabilidad, plataformas estatales o tratamiento automatizado de información. Desde la perspectiva de Avbelj (2024), el constitucionalismo necesita responder a transformaciones tecnológicas capaces de alterar sus presupuestos teóricos. En Ecuador, esa exigencia reclama interpretar los derechos atendiendo a las nuevas mediaciones técnicas del poder público actuales.

Hay, además, una transformación del espacio jurídico. La relación entre Estado y persona ya no ocurre exclusivamente ante una ventanilla, un expediente físico o una audiencia presencial. La Ley Orgánica para la Transformación Digital y Audiovisual (2023) impulsa tecnologías digitales para trámites administrativos y judiciales, trasladando parte de la actividad jurídica hacia infraestructuras electrónicas. Ese cambio modifica tiempos, evidencias, formas de acceso y expectativas ciudadanas, mientras obliga a preservar igualdad, seguridad jurídica y tutela efectiva.

La cuestión constitucional aparece con mayor intensidad cuando la técnica participa en la distribución de oportunidades, servicios o cargas. Un sistema digital puede ordenar prioridades, verificar identidades o estructurar decisiones administrativas, convirtiendo su diseño en una forma discreta de normatividad. Avbelj (2024) plantea que la sociedad algorítmica demanda una reformulación del constitucionalismo capaz de responder al poder tecnológico. Para Ecuador, ello implica someter toda mediación

digital estatal a derechos, competencias, controles y responsabilidades jurídicamente identificables.

La transformación digital tampoco puede separarse de la inclusión. El marco legal ecuatoriano vincula infraestructura, cultura digital, educación, salud y economía dentro de sus ejes regulatorios (Ley Orgánica para la Transformación Digital y Audiovisual, 2023, art. 2). Esta amplitud muestra que la digitalización atraviesa ámbitos donde se materializan derechos y políticas públicas. Cuando el acceso tecnológico es desigual, la innovación administrativa puede reproducir distancias sociales; por eso, la modernización debe conservar una vocación constitucional igualitaria.

Vista desde el constitucionalismo digital, la transformación ecuatoriana representa una mutación del sistema jurídico porque altera simultáneamente instituciones, procedimientos, fuentes de poder y condiciones materiales para ejercer derechos. El Reglamento reconoce tecnologías avanzadas, entre ellas inteligencia artificial, analítica y tecnologías cognitivas (Reglamento General a la Ley Orgánica para la Transformación Digital y Audiovisual, 2023, art. 3). Frente a este escenario, Avbelj (2024) reclama renovar la teoría constitucional para mantener jurídicamente gobernado el poder tecnológico contemporáneo.

1.2. Constitución, dignidad humana y autodeterminación en entornos digitales

La Constitución ecuatoriana sitúa a la dignidad humana como fundamento material de los derechos y límite frente al ejercicio del poder, también cuando este adopta formas digitales. En espacios gobernados por datos, perfiles y sistemas automatizados, la persona no puede reducirse a una categoría estadística. Zhao (2025) vincula la gobernanza algorítmica legítima con valores centrados en dignidad y autonomía. Esta perspectiva

permite leer la digitalización desde la primacía constitucional de la persona y sus decisiones.

Figura 2

Dignidad y autodeterminación digital



La autodeterminación adquiere especial densidad jurídica cuando la vida cotidiana deja rastros susceptibles de clasificación, inferencia y reutilización. El libre desarrollo de la personalidad reconocido constitucionalmente protege la capacidad individual de construir proyectos vitales sin interferencias arbitrarias (Constitución de la República del Ecuador, 2008, art. 66). En entornos digitales, dicha libertad exige preservar márgenes reales de decisión frente a tecnologías capaces de orientar preferencias, anticipar conductas y condicionar oportunidades mediante tratamientos intensivos de información personal.

La intimidad conserva su raíz clásica, pero su significado constitucional se amplía ante ecosistemas donde observar ya no requiere presencia física. Registros de navegación, ubicaciones, hábitos y relaciones pueden revelar dimensiones profundas de una

persona. La Constitución protege la intimidad personal y familiar (Constitución de la República del Ecuador, 2008, art. 66). Desde otra vertiente, Zhao (2025) destaca que una gobernanza algorítmica compatible con la dignidad debe impedir que la eficiencia desplace la autonomía individual.

El derecho a la protección de datos introduce una garantía de la autodeterminación digital. La Constitución reconoce a cada persona facultades respecto del acceso y decisión sobre información y datos de este carácter (Constitución de la República del Ecuador, 2008, art. 66). La Ley Orgánica de Protección de Datos Personales desarrolla esa garantía mediante principios, derechos y obligaciones. Su sentido constitucional radica en devolver capacidad de intervención al individuo frente a tratamientos informacionales potencialmente invasivos.

La dignidad no opera como una declaración ornamental dentro de la gobernanza tecnológica. Funciona como criterio para evaluar diseños, procedimientos y decisiones que afectan a personas concretas. Zhao (2025) sostiene que incorporar valores humanos en sistemas algorítmicos requiere atender la autonomía y evitar formas de instrumentalización. Esta premisa dialoga con la Constitución ecuatoriana, cuyo régimen de derechos impide tratar al individuo como objeto pasivo de procesamiento, especialmente cuando existen consecuencias relevantes para su vida personal.

El consentimiento ocupa un lugar en esta arquitectura, aunque no agota la protección constitucional. La Ley Orgánica de Protección de Datos Personales (2021) exige condiciones jurídicas para que el tratamiento responda a bases legítimas y reconoce derechos del titular sobre sus datos. En relaciones digitales marcadas por asimetrías informativas, aceptar una interfaz no equivale necesariamente a ejercer autonomía plena. La dignidad demanda opciones comprensibles, libertad decisoria y posibilidades efectivas de controlar usos posteriores de información.

Existe una tensión cuando sistemas automatizados intervienen en decisiones con efectos jurídicos o personales relevantes. La Ley Orgánica de Protección de Datos Personales (2021) reconoce garantías vinculadas con decisiones basadas en valoraciones automatizadas. Tal protección adquiere sentido constitucional al conectarse con dignidad, libertad e intimidad. Zhao (2025) plantea que la alineación entre algoritmos y valores humanos requiere estructuras de gobernanza capaces de preservar agencia individual, especialmente frente a procesos técnicos difíciles de comprender o cuestionar.

La autodeterminación digital también requiere conocimiento del tratamiento de información. Sin transparencia, la libertad puede convertirse en una fórmula vacía: nadie controla aquello cuya existencia desconoce. La Ley Orgánica de Protección de Datos Personales (2021) establece deberes de información y derechos que permiten al titular intervenir en el tratamiento. Esta arquitectura coincide con Zhao (2025), para quien la dignidad debe proyectarse sobre la gobernanza algorítmica mediante mecanismos que mantengan a la persona como referente normativo.

La protección constitucional adquiere importancia cuando la capacidad tecnológica permite inferir rasgos que la persona nunca declaró expresamente. Un conjunto de datos aparentemente ordinarios puede producir perfiles sobre preferencias, comportamientos o vulnerabilidades. Frente a ello, dignidad e intimidad actúan como límites materiales. La Constitución ecuatoriana reconoce protección de datos e intimidad (Constitución de la República del Ecuador, 2008, art. 66), mientras Zhao (2025) reclama orientar la gobernanza algorítmica hacia el respeto efectivo de la autonomía.

Constitución y legislación de datos convergen, en una idea de ciudadanía digital incompatible con la reducción de la persona a insumo informacional. La dignidad exige conservar espacios de elección, reserva y participación frente a infraestructuras

automatizadas. La Ley Orgánica de Protección de Datos Personales (2021) aporta mecanismos para ejercer control sobre información, mientras Zhao (2025) vincula la legitimidad algorítmica con valores humanos. El constitucionalismo ecuatoriano encuentra aquí una tarea: proteger autonomía dentro de la innovación.

1.3. Eficacia horizontal de los derechos constitucionales frente al poder tecnológico privado

La expansión del poder tecnológico privado obliga a revisar la lectura tradicional de los derechos constitucionales como defensas dirigidas principalmente frente al Estado. Plataformas, proveedores digitales y empresas dedicadas al tratamiento de datos ejercen capacidades capaces de afectar libertades individuales. Frosio (2023) examina esta tensión al estudiar la responsabilidad de las plataformas desde los derechos fundamentales. En Ecuador, la Constitución permite abordar tales relaciones desde una eficacia horizontal que vincula también a determinados actores particulares.

La eficacia horizontal adquiere relevancia cuando una empresa tecnológica dispone de información, infraestructura o capacidad decisoria suficiente para condicionar derechos. El artículo 88 de la Constitución admite la acción de protección frente a particulares bajo determinadas circunstancias, entre ellas daño grave, subordinación, indefensión o discriminación (Constitución de la República del Ecuador, 2008). Esta previsión rompe una frontera rígida entre poder público y privado, reconociendo que ciertas relaciones entre particulares pueden producir afectaciones constitucionalmente relevantes en espacios digitales.

El poder de las plataformas presenta una dimensión normativa difícil de ignorar. Sus reglas privadas determinan acceso, permanencia, visibilidad y circulación de contenidos, mientras sus arquitecturas técnicas distribuyen oportunidades de interacción. Frosio (2023) sostiene que la responsabilidad de intermediarios

digitales debe examinarse tomando seriamente los derechos fundamentales involucrados. Tal premisa resulta pertinente para Ecuador: la autonomía empresarial encuentra límites cuando decisiones privadas interfieren de manera intensa con libertades, dignidad, igualdad o protección informacional de sus usuarios.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional desarrolla la tutela frente a particulares cuando concurren condiciones constitucionalmente relevantes. La acción de protección procede ante vulneraciones provenientes de personas privadas en los casos previstos por el ordenamiento (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009, art. 41). Trasladada al ámbito tecnológico, esta garantía ofrece una vía para discutir actuaciones privadas que, debido a su intensidad, produzcan indefensión, discriminación o daños graves sobre derechos constitucionales de personas.

La protección de datos revela con claridad esta proyección horizontal. Buena parte del tratamiento informacional contemporáneo ocurre dentro de relaciones privadas, desde servicios digitales hasta plataformas comerciales. La Ley Orgánica de Protección de Datos Personales (2021) establece obligaciones para responsables y encargados, junto con derechos exigibles por sus titulares. La Constitución, por su parte, reconoce el derecho a la protección de datos personales (Constitución de la República del Ecuador, 2008, art. 66), reforzando límites frente al poder informacional empresarial.

Sin embargo, reconocer derechos frente a empresas tecnológicas no significa trasladar mecánicamente categorías diseñadas para relaciones estatales. Existen libertades concurrentes que también merecen protección, entre ellas iniciativa económica, propiedad y libertad de expresión. Frosio (2023) muestra que la regulación de plataformas requiere ponderar derechos potencialmente enfrentados dentro de estructuras privadas. El constitucionalismo ecuatoriano debe atender esa pluralidad,

evitando que la protección de una posición jurídica elimine injustificadamente otras facultades igualmente reconocidas por el orden constitucional vigente.

La transformación digital añade otra capa al problema porque incrementa la dependencia social respecto de infraestructuras administradas por particulares. La Ley Orgánica para la Transformación Digital y Audiovisual (2023) promueve la adopción tecnológica en actividades públicas y privadas. Cuando servicios digitales adquieren importancia para trabajar, comunicarse o participar económicamente, las condiciones impuestas por proveedores dejan de tener efectos meramente contractuales. Algunas decisiones empresariales pueden alcanzar una intensidad material que justifique examinarlas bajo parámetros constitucionales de protección.

Frosio (2023) advierte que la gobernanza de plataformas debe incorporar los derechos fundamentales dentro de los propios regímenes de responsabilidad. Esta perspectiva desplaza la discusión desde una pregunta centrada en la legalidad formal hacia otra vinculada con los efectos concretos de las decisiones tecnológicas. En Ecuador, semejante enfoque encuentra respaldo en la aplicación directa de derechos y garantías constitucionales, particularmente cuando la posición dominante de un particular reduce las posibilidades reales de defensa de una persona afectada.

La eficacia horizontal requiere, además, distinguir influencia económica de poder constitucionalmente relevante. No toda controversia con una empresa tecnológica constituye vulneración de derechos. La Constitución ecuatoriana establece condiciones específicas para activar garantías frente a particulares (Constitución de la República del Ecuador, 2008, art. 88). Esta cautela resulta necesaria para preservar el carácter jurídico de la tutela constitucional. El análisis debe valorar intensidad de la afectación, asimetría entre las partes y posibilidades efectivas de protección ordinaria disponibles.

El constitucionalismo digital ecuatoriano encuentra aquí una frontera en movimiento. El poder privado puede organizar espacios de comunicación, procesar información personal y adoptar decisiones con consecuencias significativas para derechos individuales. Frosio (2023) permite comprender que las plataformas deben asumir responsabilidades compatibles con los derechos fundamentales. La Constitución, la legislación de datos y las garantías jurisdiccionales ofrecen herramientas para responder a esas relaciones, procurando que innovación y autonomía privada permanezcan vinculadas al respeto efectivo de la persona humana.

1.4. Identidad digital, personalidad jurídica y construcción del sujeto en el ecosistema algorítmico

La identidad digital transforma la manera en que el derecho reconoce a la persona dentro de relaciones mediadas por tecnología. Nombre, credenciales, datos biométricos, historiales y patrones conductuales componen representaciones capaces de adquirir efectos jurídicos propios. Vardanyan et al. (2024) vinculan esta fragmentación identitaria con problemas de integridad y autodeterminación informativa. En Ecuador, la cuestión adquiere dimensión constitucional porque identidad, intimidad y protección de datos convergen alrededor de una persona cuya presencia digital permanece jurídicamente protegida.

La Constitución reconoce el derecho a la identidad personal y colectiva, junto con atributos vinculados al nombre, características materiales e inmateriales y procedencia familiar (Constitución de la República del Ecuador, 2008, art. 66). En espacios digitales, tales elementos conviven con identificadores creados por sistemas informáticos. La identidad jurídica deja entonces de descansar enteramente en registros tradicionales. Aparecen representaciones derivadas de datos que pueden condicionar reconocimiento, acceso a servicios y ejercicio de derechos en múltiples relaciones contemporáneas.

Esta multiplicación de representaciones plantea una diferencia relevante entre personalidad jurídica e identidad digital. La primera expresa el reconocimiento de la persona como titular de derechos y obligaciones; la segunda articula datos mediante los cuales sistemas tecnológicos identifican, autentican o clasifican individuos. Vardanyan et al. (2024) advierten que la fragmentación digital puede afectar integridad personal y autodeterminación informativa. El derecho ecuatoriano debe impedir que perfiles computacionales sustituyan indebidamente la identidad jurídicamente reconocida del individuo ante terceros.

La Ley Orgánica de Protección de Datos Personales ofrece herramientas para preservar esa correspondencia entre persona e información. Sus principios regulan tratamientos realizados sobre datos vinculados o vinculables con individuos y reconocen facultades de acceso, rectificación, actualización y eliminación (Ley Orgánica de Protección de Datos Personales, 2021). Estas garantías adquieren especial relevancia cuando una identidad digital contiene errores. Una clasificación incorrecta puede acompañar silenciosamente al individuo, replicarse entre sistemas y afectar decisiones posteriores sobre su persona.

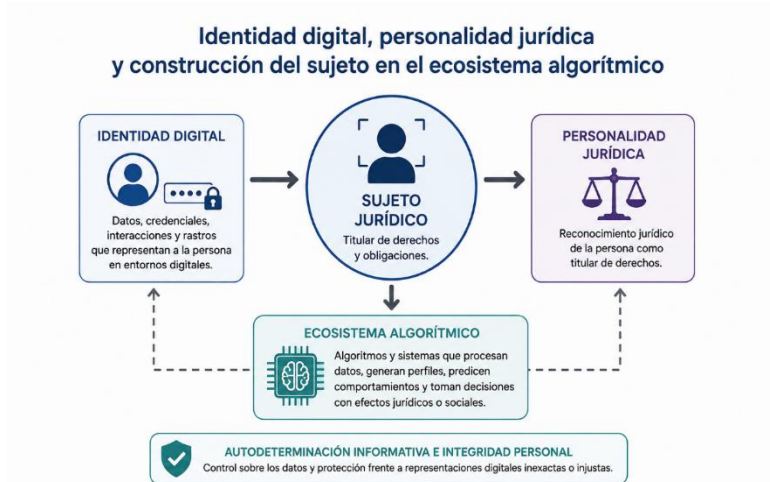
La identidad digital también cumple una función probatoria dentro de intercambios jurídicos electrónicos. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2002) reconoce efectos jurídicos a mensajes de datos y regula mecanismos de firma electrónica vinculados con identificación y autenticación. Esta arquitectura permite trasladar actos jurídicamente relevantes al espacio digital. Sin embargo, autenticar una voluntad no equivale a definir integralmente a quien la expresa: la personalidad humana desborda cualquier credencial técnica utilizada para identificarla.

En el ecosistema algorítmico, la identidad puede construirse mediante inferencias que la persona nunca formuló acerca de sí misma. Preferencias, probabilidades y categorías

atribuidas forman perfiles paralelos con capacidad para orientar decisiones. Vardanyan et al. (2024) relacionan este fenómeno con la necesidad de preservar integridad identitaria y control informacional. Desde la Constitución ecuatoriana, la protección de datos personales ofrece un límite frente a representaciones digitales capaces de alterar la percepción institucional o comercial del individuo.

Figura 3

Configuración jurídica de la identidad digital



La autodeterminación informativa adquiere entonces una dimensión vinculada con la propia narrativa personal. Controlar datos significa también intervenir en las representaciones que terceros construyen mediante ellos. La Ley Orgánica de Protección de Datos Personales (2021) reconoce derechos destinados a conocer y modificar determinados tratamientos informacionales. Tales facultades permiten resistir identidades digitales rígidas o inexactas. Vardanyan et al. (2024) destacan que preservar la integridad personal requiere atender la relación entre fragmentación digital, privacidad y autonomía del individuo.

La transformación digital institucionaliza además mecanismos de identificación necesarios para relacionarse con administraciones y prestadores privados. La Ley Orgánica para la Transformación Digital y Audiovisual (2023) impulsa servicios, trámites y procedimientos mediante tecnologías digitales. Este proceso amplía posibilidades de interacción, aunque también vuelve determinante la confiabilidad de los sistemas identificatorios. Una credencial comprometida, un dato desactualizado o una asociación errónea pueden impedir ejercer derechos, realizar gestiones o acreditar jurídicamente actuaciones atribuibles a una persona determinada.

El problema adquiere mayor profundidad cuando perfiles algorítmicos producen versiones fragmentadas de una misma persona. Un individuo puede aparecer como consumidor ante una plataforma, riesgo ante otra organización y titular de derechos ante el Estado. Vardanyan et al. (2024) examinan precisamente la tensión entre esas identidades parciales y la integridad individual. El constitucionalismo ecuatoriano debe mantener una premisa básica: ninguna clasificación tecnológica puede absorber la complejidad jurídica, biográfica y moral de la personalidad humana plenamente reconocida.

La construcción digital del sujeto exige, por tanto, conectar innovación tecnológica con una concepción constitucional de persona. Identificación electrónica, tratamiento de datos y perfiles algorítmicos pueden facilitar relaciones jurídicas, pero también alterar la representación social del individuo. La Constitución y la legislación ecuatoriana proporcionan garantías para preservar identidad, intimidad y control informacional. Desde Vardanyan et al. (2024), esta protección adquiere sentido adicional: defender la integridad identitaria significa conservar continuidad personal frente a representaciones digitales fragmentarias.

1.5. Ciudadanía digital y nuevas formas de participación, interacción y ejercicio democrático

La ciudadanía digital expresa una transformación de las formas mediante las cuales las personas participan en asuntos públicos, deliberan y construyen posiciones políticas. Las tecnologías amplían espacios de interacción, pero también modifican capacidades necesarias para intervenir responsablemente. Gonzalez-Mohino et al. (2023) vinculan las herramientas digitales con el pensamiento crítico y la participación ciudadana. En Ecuador, esta relación encuentra fundamento constitucional en los derechos de participación, cuyo ejercicio puede proyectarse hacia escenarios tecnológicos sin perder su dimensión democrática.

La Constitución concibe la participación como derecho ejercido mediante mecanismos de democracia representativa, directa y comunitaria (Constitución de la República del Ecuador, 2008, art. 95). La digitalización agrega canales para expresar opiniones, organizar iniciativas y relacionarse con instituciones públicas. Estas posibilidades no reemplazan las formas constitucionales existentes; modifican sus condiciones materiales de ejercicio. La ciudadanía adquiere una presencia digital desde la cual puede deliberar, fiscalizar y participar, siempre bajo garantías compatibles con igualdad y libertad.

El acceso a información pública ocupa una posición central en esta arquitectura democrática. La Constitución garantiza buscar, recibir, intercambiar, producir y difundir información, además del acceso libre a aquella generada por entidades públicas (Constitución de la República del Ecuador, 2008, arts. 18 y 91). En espacios digitales, la disponibilidad informativa puede fortalecer la vigilancia ciudadana sobre decisiones estatales. Sin embargo, disponer de información no basta: comprenderla críticamente

constituye una condición relevante para ejercer participación democrática significativa.

Gonzalez-Mohino et al. (2023) encuentran una relación entre herramientas digitales, aprendizaje colaborativo y desarrollo del pensamiento crítico necesario para la participación ciudadana. Esta conexión resulta especialmente pertinente cuando el debate político circula por plataformas caracterizadas por velocidad, fragmentación y abundancia informativa. La ciudadanía digital requiere capacidades para contrastar argumentos, reconocer fuentes y elaborar juicios propios. Sin estas competencias, la ampliación tecnológica de la conversación pública puede incrementar intervenciones ciudadanas sin fortalecer necesariamente la calidad deliberativa democrática.

La participación electoral también experimenta cambios derivados de la comunicación digital. El Código de la Democracia regula procesos electorales, organizaciones políticas, promoción electoral y condiciones destinadas a preservar la voluntad ciudadana (Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, 2009). Redes y plataformas añaden nuevas formas de circulación del discurso político. Su influencia obliga a considerar transparencia, igualdad electoral e información como componentes vinculados con elecciones democráticamente libres.

La ciudadanía digital no termina en las urnas. Comprende interacción permanente con instituciones, acceso a servicios, deliberación pública y capacidad de formular demandas colectivas mediante canales tecnológicos. La Ley Orgánica para la Transformación Digital y Audiovisual (2023) impulsa medios digitales en la prestación de servicios y actuaciones estatales. Esta orientación puede acercar administración y ciudadanía cuando los canales tecnológicos facilitan gestiones y comunicación. Su legitimidad democrática depende, sin embargo, de accesibilidad, confianza y posibilidades efectivas de participación.

Existe una dimensión igualitaria que merece atención. Cuando el ejercicio ciudadano depende crecientemente de conectividad, dispositivos y competencias digitales, las desigualdades tecnológicas pueden convertirse en desigualdades democráticas. La Constitución reconoce el acceso universal a tecnologías de información y comunicación (Constitución de la República del Ecuador, 2008, art. 16). Gonzalez-Mohino et al. (2023) destacan el valor educativo de herramientas digitales para fortalecer capacidades participativas. Garantizar acceso requiere, entonces, acompañarlo con formación crítica y oportunidades reales de intervención.

Las plataformas digitales también transforman la temporalidad de la participación. Opiniones, convocatorias y demandas circulan con una rapidez desconocida para mecanismos institucionales tradicionales. Esta inmediatez puede acercar voces ciudadanas al debate público, aunque también favorecer respuestas impulsivas y discursos escasamente reflexivos. Gonzalez-Mohino et al. (2023) resaltan la importancia del pensamiento crítico dentro de experiencias participativas mediadas tecnológicamente. La democracia digital necesita espacios donde velocidad y deliberación encuentren un equilibrio respetuoso de pluralidad y razonamiento público.

La transformación tecnológica modifica, además, la relación entre ciudadanía y representación política. Los representantes pueden comunicarse directamente con electores, mientras estos disponen de herramientas para observar actuaciones, cuestionarlas y organizar respuestas colectivas. El Código de la Democracia estructura la participación política dentro del sistema electoral ecuatoriano, mientras la Constitución reconoce fiscalización y participación ciudadana (Constitución de la República del Ecuador, 2008, arts. 61 y 95). La tecnología añade nuevas vías para ejercer esas facultades democráticas.

La ciudadanía digital ecuatoriana debe comprenderse como prolongación de la ciudadanía constitucional dentro de relaciones tecnológicamente mediadas. Participar digitalmente exige derechos, acceso, competencias críticas y garantías frente a exclusiones. Gonzalez-Mohino et al. (2023) permiten vincular herramientas digitales con capacidades ciudadanas orientadas hacia una participación reflexiva. La Constitución, el Código de la Democracia y la legislación sobre transformación digital aportan bases para una democracia donde innovación tecnológica fortalezca deliberación, control público y presencia ciudadana efectiva.

1.6. Jurisdicción, territorialidad y soberanía estatal ante infraestructuras digitales transnacionales

La infraestructura digital transnacional altera la relación histórica entre derecho, territorio y autoridad estatal. Datos generados en Ecuador pueden almacenarse, procesarse o transferirse mediante servidores ubicados bajo jurisdicciones diferentes, mientras las decisiones tecnológicas producen efectos inmediatos sobre residentes ecuatorianos. Fahey (2023) relaciona soberanía digital y protección de datos con debates acerca de localización y circulación informacional. Esta realidad exige reconsiderar la territorialidad jurídica sin abandonar la capacidad constitucional del Estado para proteger derechos dentro de sus competencias.

La Constitución afirma que la soberanía radica en el pueblo y establece al territorio ecuatoriano como unidad geográfica e histórica sometida al orden estatal (Constitución de la República del Ecuador, 2008, arts. 1 y 4). Sin embargo, las infraestructuras digitales atraviesan fronteras mediante operaciones técnicamente distribuidas. El problema jurídico aparece cuando territorio físico y espacio de procesamiento dejan de coincidir. Determinar la norma

aplicable requiere atender vínculos efectivos entre tratamiento, personas afectadas y jurisdicción competente.

La Ley Orgánica de Protección de Datos Personales adopta criterios territoriales capaces de proyectar obligaciones más allá del establecimiento físico del responsable. Su ámbito comprende determinados tratamientos vinculados con titulares residentes en Ecuador, incluso cuando intervienen responsables o encargados establecidos fuera del país (Ley Orgánica de Protección de Datos Personales, 2021, art. 2). Esta fórmula responde a una realidad evidente: trasladar infraestructura al extranjero no puede convertirse en mecanismo para sustraer tratamientos de garantías jurídicas nacionales.

La territorialidad digital se construye, entonces, mediante conexiones jurídicas que trascienden la ubicación del servidor. Importan el domicilio del titular, los efectos del tratamiento y la oferta de bienes o servicios dirigida hacia personas situadas en Ecuador. El Reglamento General desarrolla obligaciones aplicables a responsables y encargados no establecidos en territorio nacional (Reglamento General a la Ley Orgánica de Protección de Datos Personales, 2023). Con ello, la jurisdicción procura seguir relaciones informacionales antes que fronteras estrictamente físicas.

Fahey (2023) observa que la soberanía digital mantiene una relación compleja con políticas de localización de datos. Proteger capacidad regulatoria no equivale necesariamente a exigir que toda información permanezca físicamente dentro del territorio nacional. Para Ecuador, esta distinción resulta relevante. La soberanía puede expresarse mediante reglas sobre tratamiento, responsabilidad y garantías exigibles, aun cuando la infraestructura se encuentre distribuida internacionalmente. El objetivo jurídico reside en conservar autoridad efectiva frente a operaciones tecnológicas vinculadas con derechos nacionales.

Las transferencias internacionales muestran con especial claridad esa tensión. La Ley Orgánica de Protección de Datos Personales (2021) regula el flujo transfronterizo procurando que la movilidad de información no elimine las garantías reconocidas al titular. El Reglamento General desarrolla mecanismos aplicables a estas operaciones (Reglamento General a la Ley Orgánica de Protección de Datos Personales, 2023). La circulación internacional resulta jurídicamente admisible cuando conserva niveles de protección compatibles con el ordenamiento ecuatoriano y permite atribuir responsabilidades verificables.

La jurisdicción estatal enfrenta una dificultad práctica cuando el responsable extranjero carece de presencia material en Ecuador. Una norma puede declarar obligaciones, pero su eficacia depende de mecanismos que permitan supervisar tratamientos, exigir cumplimiento y ejecutar decisiones. El Reglamento General contempla reglas dirigidas a responsables y encargados no establecidos en Ecuador, reforzando la proyección extraterritorial del régimen nacional. Fahey (2023) permite advertir que soberanía digital significa también capacidad institucional para convertir pretensiones regulatorias en protección jurídicamente efectiva.

La soberanía digital tampoco debe confundirse con aislamiento tecnológico. Internet funciona mediante redes, servicios y cadenas de procesamiento distribuidas entre numerosos territorios. Fahey (2023) analiza precisamente las tensiones entre autonomía regulatoria, circulación de datos y tendencias hacia su localización. Ecuador necesita preservar su potestad normativa mientras participa en intercambios digitales transfronterizos. La cuestión consiste en evitar que apertura tecnológica equivalga a renuncia jurisdiccional, especialmente cuando están comprometidos privacidad, protección informacional y demás derechos constitucionales de residentes.

La Constitución reconoce el derecho a la protección de datos personales y exige autorización del titular o mandato legal

para su tratamiento en los términos establecidos jurídicamente (Constitución de la República del Ecuador, 2008, art. 66). Esta garantía no pierde fuerza porque la información atraviese una frontera. Su proyección internacional obliga al Estado a desarrollar instrumentos regulatorios capaces de acompañar jurídicamente los datos cuando circulan mediante infraestructuras extranjeras, preservando derechos frente a responsables ubicados fuera del territorio.

Jurisdicción, territorialidad y soberanía adquieren nuevos significados cuando las infraestructuras digitales separan ubicación física, tratamiento y efectos jurídicos. Fahey (2023) muestra que la soberanía digital puede articularse mediante regulación de flujos informacionales sin reducirse a políticas estrictas de localización. El régimen ecuatoriano adopta una orientación compatible con esa lógica al extender garantías y obligaciones hacia ciertos tratamientos transnacionales. La soberanía constitucional reside, entonces, en mantener derechos exigibles allí donde circulen datos vinculados con Ecuador.

Tabla 1
Dimensiones del constitucionalismo digital y su proyección en el orden jurídico ecuatoriano

Dimensión constitucional	Proyección jurídica en el entorno digital ecuatoriano
Transformación digital del sistema jurídico	La incorporación progresiva de tecnologías digitales modifica procedimientos, servicios, relaciones jurídicas y formas de ejercicio del poder. La Constitución y la legislación sobre transformación digital proporcionan parámetros para integrar innovación tecnológica con juridicidad, derechos fundamentales y responsabilidad institucional.
Dignidad humana y autodeterminación	La dignidad constituye un límite material frente al tratamiento intensivo de datos y las decisiones automatizadas. La autonomía, el libre desarrollo de la personalidad, la intimidad y la protección de datos adquieren especial relevancia cuando sistemas

Dimensión constitucional	Proyección jurídica en el entorno digital ecuatoriano
	algorítmicos intervienen en decisiones que afectan la esfera individual.
Eficacia horizontal de los derechos	El poder tecnológico privado puede producir afectaciones constitucionalmente relevantes. Plataformas, proveedores y responsables del tratamiento de datos quedan sujetos a obligaciones jurídicas destinadas a proteger derechos, particularmente cuando existen relaciones de subordinación, indefensión, discriminación o asimetría significativa.
Identidad digital y personalidad jurídica	Datos, credenciales, perfiles e inferencias algorítmicas generan representaciones digitales de la persona. El ordenamiento debe preservar la identidad, integridad personal y autodeterminación informativa, evitando que clasificaciones tecnológicas inexactas o fragmentarias sustituyan indebidamente la personalidad jurídicamente reconocida.
Ciudadanía y participación digital	Las tecnologías amplían canales de deliberación, información, fiscalización e intervención ciudadana. Su dimensión constitucional exige garantizar acceso, igualdad, pensamiento crítico y participación efectiva, procurando que la digitalización fortalezca el ejercicio democrático sin profundizar brechas tecnológicas o informativas.
Jurisdicción, territorialidad y soberanía digital	La circulación transfronteriza de datos obliga a reconsiderar la relación entre territorio y jurisdicción. El régimen ecuatoriano proyecta determinadas garantías hacia tratamientos realizados fuera del país cuando mantienen vínculos jurídicamente relevantes con Ecuador, preservando capacidad regulatoria y protección efectiva de derechos.

Nota. La tabla articula los ejes desarrollados en el Capítulo 1 a partir de Avbelj (2024), Zhao (2025), Frosio (2023), Vardanyan et al. (2024), Gonzalez-Mohino et al. (2023) y Fahey (2023), en relación con la Constitución de la República del Ecuador y la normativa ecuatoriana examinada en cada apartado.

Capítulo 2:

Inteligencia artificial, decisión algorítmica y responsabilidad jurídica

La inteligencia artificial ha dejado de ocupar un espacio periférico en la reflexión jurídica para instalarse entre las cuestiones que interpelan directamente al Estado, las empresas y la ciudadanía. Sus sistemas clasifican información, recomiendan acciones, generan contenidos y participan en decisiones capaces de producir consecuencias jurídicas. Zaidan e Ibrahim (2024) advierten que esta expansión tecnológica ocurre dentro de escenarios regulatorios complejos, donde las instituciones deben responder con capacidad técnica, coordinación normativa y mecanismos de gobernanza suficientemente adaptables.

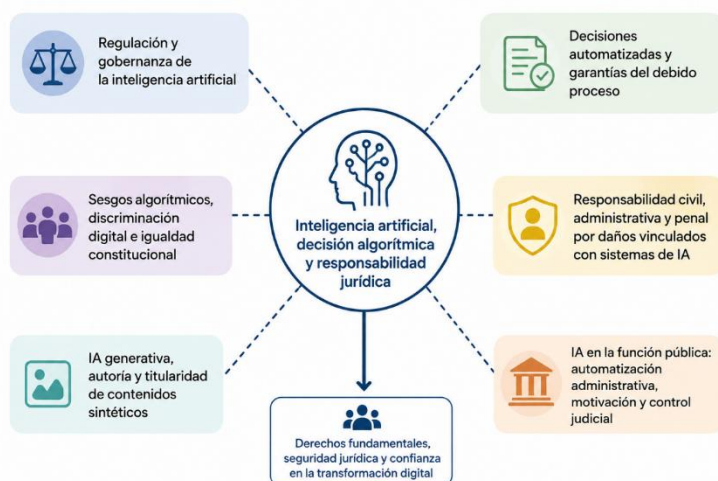
El derecho ecuatoriano enfrenta esta transformación desde categorías construidas alrededor de decisiones humanas, autoridades identificables y relaciones causales relativamente reconocibles. La inteligencia artificial altera parcialmente esas coordenadas. Un resultado algorítmico puede provenir de datos históricos, instrucciones humanas, modelos probabilísticos y decisiones empresariales distribuidas. Rudolf y Kovač (2024) señalan que la automatización administrativa modifica relaciones tradicionales entre actuación pública, protección de datos y garantías procedimentales, obligando a reconsiderar los instrumentos destinados a controlar jurídicamente el ejercicio del poder.

Esta tensión adquiere especial intensidad cuando un algoritmo participa en decisiones que afectan derechos. La rapidez computacional puede aportar eficiencia, pero una resolución difícil de comprender compromete defensa, contradicción y motivación. Rudolf y Kovač (2024) destacan que los sistemas automatizados requieren salvaguardias compatibles con los principios del derecho administrativo y la protección de datos. En Ecuador, tales exigencias dialogan con garantías constitucionales que reclaman decisiones motivadas, seguridad jurídica y procedimientos capaces de ofrecer respuestas comprensibles a las personas afectadas.

La aparente neutralidad matemática tampoco elimina las desigualdades presentes en los datos utilizados por sistemas inteligentes. Un algoritmo puede reproducir patrones discriminatorios sin recurrir expresamente a categorías protegidas, mediante correlaciones o variables indirectas. Kelly-Lyth (2023) demuestra que este problema adquiere particular relevancia en el ámbito laboral, donde herramientas automatizadas intervienen en contratación y evaluación. La igualdad constitucional exige, por ello, observar resultados materiales, identificar impactos diferenciados y evitar que la discriminación encuentre refugio bajo una apariencia tecnológica objetiva.

Figura 4

Estructura jurídica de la inteligencia artificial



Junto con la discriminación aparece una pregunta inevitable: quién responde cuando la inteligencia artificial causa un daño. La respuesta pierde sencillez cuando desarrolladores, proveedores, operadores y usuarios participan en distintas etapas del funcionamiento tecnológico. Al-Dulaimi (2025) explica que la autonomía de ciertos sistemas tensiona los modelos tradicionales

de imputación, especialmente en el sector público. El problema jurídico consiste entonces en distribuir responsabilidad atendiendo al control efectivo, la conducta desplegada, los deberes incumplidos y la relación causal jurídicamente demostrable.

Las consecuencias pueden proyectarse sobre diversos regímenes de responsabilidad. Un daño algorítmico puede generar obligaciones civiles de reparación, responsabilidad administrativa, infracciones vinculadas con datos personales e incluso consecuencias penales cuando concurren los elementos exigidos legalmente. Al-Dulaimi (2025) destaca que la atribución requiere distinguir cuidadosamente la participación humana respecto del funcionamiento autónomo del sistema. Esta perspectiva resulta especialmente pertinente para Ecuador, donde cada régimen conserva presupuestos propios que no deberían diluirse por la complejidad técnica de la inteligencia artificial.

La inteligencia artificial generativa incorpora otra dimensión: la producción de textos, imágenes, composiciones y expresiones sintéticas cuestiona categorías de autoría construidas alrededor de creatividad humana. Neubauer et al. (2026) sitúan la originalidad personal como elemento determinante para examinar la protección autoral ante contenidos generados mediante sistemas inteligentes. La cuestión excede la propiedad intelectual. También obliga a pensar la relación entre instrucciones, selección, edición y control creativo, especialmente cuando la intervención humana aparece entrelazada con procesos computacionales probabilísticos complejos.

Quintais (2025) amplía esta discusión al estudiar las tensiones entre inteligencia artificial generativa y derecho de autor, particularmente respecto del entrenamiento de modelos y los contenidos producidos. En Ecuador, estas cuestiones dialogan con el Código Ingenios y con relaciones contractuales establecidas entre usuarios y proveedores tecnológicos. Determinar autoría y titularidad requiere distinguir creación humana, producción

algorítmica y transferencia patrimonial, evitando atribuir automáticamente protección jurídica a resultados cuya originalidad personal no pueda identificarse de manera jurídicamente relevante.

La función pública constituye, quizá, el espacio donde estas preguntas convergen con mayor intensidad. Automatizar procedimientos puede mejorar tiempos y capacidad institucional, pero también introducir opacidad dentro de decisiones sometidas a legalidad y control jurisdiccional. Ameen (2026) sostiene que la revisión judicial de sistemas administrativos algorítmicos debe atender legalidad, equidad y rendición de cuentas. Ninguna herramienta tecnológica debería convertir una actuación estatal en una decisión inaccesible para quien necesita comprenderla, controvertirla o solicitar su revisión judicial efectiva.

Este capítulo aborda la inteligencia artificial desde esa relación cambiante entre innovación tecnológica y responsabilidad jurídica. Zaidan e Ibrahim (2024) permiten comprender la dimensión regulatoria; Rudolf y Kovač (2024), las garantías frente a automatización; Kelly-Lyth (2023), la discriminación algorítmica; Al-Dulaimi (2025), la imputación de daños; Neubauer et al. (2026) y Quintais (2025), la autoría; mientras Ameen (2026) aporta elementos para examinar control judicial, ofreciendo una lectura articulada desde el ordenamiento jurídico ecuatoriano contemporáneo.

2.1. Inteligencia artificial y capacidad regulatoria del ordenamiento jurídico ecuatoriano

La capacidad regulatoria ecuatoriana frente a la inteligencia artificial parte de una arquitectura de transformación digital, en proceso de especialización. La Ley Orgánica para la Transformación Digital y Audiovisual (Asamblea Nacional del Ecuador, 2023) promueve tecnologías digitales, mejora regulatoria y servicios digitalizados, ofreciendo una base para gobernar sistemas algorítmicos. Sin embargo, regular inteligencia artificial

exige coordinación técnica, jurídica y administrativa, pues la velocidad tecnológica rebasa con frecuencia los ritmos ordinarios de producción normativa nacional.

El Reglamento General a la Ley Orgánica para la Transformación Digital y Audiovisual (Presidencia de la República del Ecuador, 2023) desarrolla procedimientos para aplicar la política digital y vincula la mejora regulatoria con transparencia y seguridad jurídica. Esa orientación importa cuando la administración incorpora algoritmos en trámites o servicios. La capacidad estatal no depende de expedir reglas; requiere instituciones capaces de comprender sistemas técnicos, evaluar riesgos, documentar decisiones y exigir responsabilidades ante afectaciones de derechos.

La experiencia comparada muestra que gobernar inteligencia artificial demanda estructuras adaptativas y coordinación entre niveles regulatorios. Zaidan e Ibrahim (2024) advierten que los Estados actúan dentro de un entorno tecnológico transnacional, cambiante y atravesado por actores privados con capacidad técnica. Para Ecuador, esta observación obliga a pensar la regulación más allá de una ley especializada: importan competencias institucionales, mecanismos de cooperación, conocimiento experto y procedimientos que permitan revisar las respuestas públicas frente al cambio tecnológico.

El Acuerdo MINTEL-MINTEL-2023-0019 (MINTEL, 2023) introdujo una pieza al disponer acciones para crear el Comité de Inteligencia Artificial, concebido como mecanismo de consulta, coordinación y articulación. Su función busca promover, seguir y evaluar estrategias en esta materia. La decisión resulta coherente con la Ley de Transformación Digital, porque traslada la gobernanza algorítmica desde declaraciones generales hacia una instancia administrativa llamada a conectar entidades, sectores y conocimientos diversos en una tecnología que desborda competencias tradicionales.

La reciente creación del Comité revela una cuestión de fondo: la regulación de inteligencia artificial necesita capacidad institucional antes que abundancia normativa. Un ordenamiento puede reconocer principios ambiciosos y, pese a ello, fracasar cuando las autoridades carecen de recursos técnicos, personal especializado o canales de cooperación. Zaidan e Ibrahim (2024) destacan que la gobernanza eficaz depende de arreglos institucionales capaces de responder a transformaciones rápidas, coordinar intereses múltiples y operar dentro de marcos regulatorios interdependientes.

La Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la Inteligencia Artificial en Ecuador, EFIA-EC 2025–2029, amplía capacidad mediante una ruta de política. Oficializada por el Acuerdo Ministerial MINTEL-MINTEL-2025-0030 (MINTEL, 2025), articula gobernanza, tecnología y adopción tecnológica responsable. Su valor político reside en ordenar prioridades estatales, vincular derechos con innovación y ofrecer criterios para que las instituciones públicas desarrollen prácticas de transparencia, supervisión humana, gestión de riesgos y protección de datos.

La capacidad regulatoria debe medirse por la posibilidad de convertir principios en controles verificables. En decisiones algorítmicas estatales, transparencia no equivale a publicar código, sino a permitir que una persona conozca las razones de la actuación, identifique responsabilidades y disponga de vías de revisión. La EFIA-EC (MINTEL, 2025) coloca la supervisión humana y el enfoque de riesgos en su eje de gobernanza, orientación compatible con una administración pública sometida a legalidad y rendición de cuentas.

Existe, además, una tensión entre innovación y protección jurídica. Una regulación rígida puede perder vigencia frente a cambios técnicos acelerados, mientras una regulación abierta puede trasladar decisiones sensibles hacia proveedores

tecnológicos sin controles suficientes. Zaidan e Ibrahim (2024) plantean que la gobernanza requiere respuestas flexibles, coordinación internacional y aprendizaje institucional. Para Ecuador, el equilibrio razonable pasa por reglas generales exigibles, estándares técnicos actualizables y autoridades con facultades reales para supervisar usos algorítmicos de alto impacto.

Desde esta perspectiva, la Ley de Transformación Digital, su Reglamento, el Comité de Inteligencia Artificial y la EFIA-EC forman capas regulatorias complementarias. La ley (Asamblea Nacional del Ecuador, 2023) aporta habilitación y principios transformadores; el reglamento desarrolla procedimientos; el Comité ofrece articulación institucional; la estrategia fija prioridades. El problema aparece cuando esas capas no dialogan entre sí. La capacidad regulatoria depende de competencias claras, coordinación administrativa, presupuesto, formación especializada y mecanismos públicos de evaluación periódica.

Ecuador dispone de una base institucional que permite avanzar hacia una gobernanza de inteligencia artificial precisa, aunque su eficacia dependerá de la implementación. La cuestión no consiste en acumular instrumentos, sino en lograr que cada entidad pueda identificar riesgos, justificar decisiones automatizadas, proteger derechos y corregir fallas. Como sostienen Zaidan e Ibrahim (2024), la regulación de tecnologías transnacionales requiere adaptación y cooperación. En el ámbito ecuatoriano, esa tarea exige convertir política digital en capacidad comprobable.

2.2. Decisiones automatizadas, explicabilidad algorítmica y garantías del debido proceso

Las decisiones automatizadas plantean una transformación relevante para el derecho administrativo, porque trasladan parte del razonamiento institucional hacia sistemas capaces de procesar datos y producir resultados con incidencia jurídica. Rudolf y Kovač (2024) sostienen que esta incorporación tecnológica modifica las

condiciones tradicionales de actuación administrativa y reclama salvaguardias apropiadas. En Ecuador, cualquier automatización estatal debe respetar los derechos constitucionales que disciplinan el ejercicio del poder público, particularmente debido proceso, motivación y seguridad jurídica de las personas.

El debido proceso constituye un límite jurídico frente a decisiones automatizadas que afecten derechos, intereses o situaciones jurídicas individuales. La Constitución de la República del Ecuador (2008, art. 76) reconoce garantías aplicables a procedimientos donde se determinen derechos y obligaciones. Tal mandato adquiere especial relevancia cuando interviene un algoritmo, pues la persona necesita conocer los elementos considerados, controvertir información incorrecta y obtener revisión efectiva. La tecnología administrativa no desplaza estas garantías; obliga a reforzar su cumplimiento material.

La motivación adquiere una dimensión particular cuando la decisión pública depende de modelos algorítmicos difíciles de interpretar. La Constitución ecuatoriana exige que las resoluciones de los poderes públicos sean debidamente motivadas, relacionando normas y hechos pertinentes (Constitución de la República del Ecuador, 2008, art. 76). Un resultado automatizado carente de explicación comprensible puede impedir la defensa del administrado. Explicar exige traducir la lógica técnica a razones jurídicas inteligibles, verificables y susceptibles de contradicción por cualquier persona afectada.

Esta exigencia guarda relación con el Código Orgánico Administrativo, que somete la actividad administrativa a principios jurídicos y establece requisitos para la motivación del acto administrativo. El Código Orgánico Administrativo (2017) demanda que las decisiones expresen normas aplicables, hechos relevantes y pertinencia del régimen jurídico invocado. Cuando participa inteligencia artificial, la administración conserva dicha responsabilidad. No basta atribuir el resultado al sistema utilizado,

pues la competencia decisoria permanece vinculada al órgano público y a sus funcionarios responsables.

La explicabilidad algorítmica debe comprenderse como una garantía instrumental para ejercer defensa y contradicción. Rudolf y Kovač (2024) observan que la automatización administrativa plantea interrogantes vinculados con transparencia, protección de datos y posibilidades efectivas de revisión. Desde una perspectiva jurídica ecuatoriana, explicar una decisión implica ofrecer información suficiente acerca de los factores determinantes, datos empleados y criterios relevantes. La explicación debe permitir reconstruir razonablemente la decisión, sin convertir el procedimiento administrativo en una descripción técnica incomprensible.

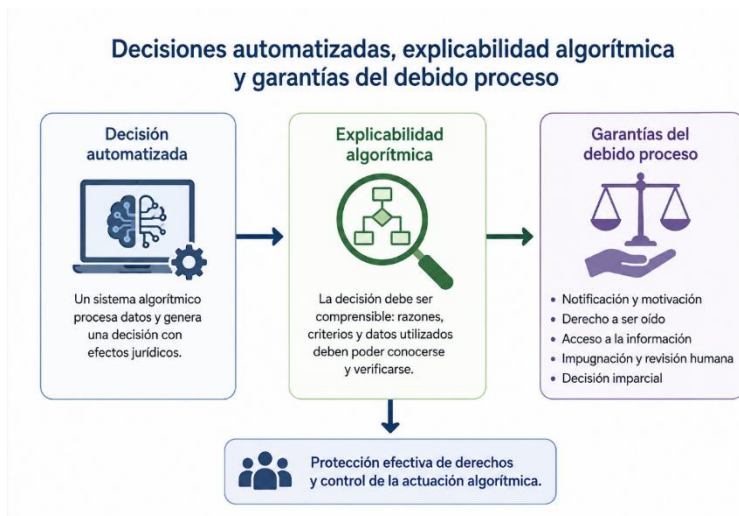
La Ley Orgánica de Protección de Datos Personales incorpora garantías específicas frente al tratamiento automatizado. Entre los derechos del titular figura no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o afecten derechos y libertades (LOPD, 2021, art. 20). Esta previsión fortalece la posición de la persona ante sistemas de inteligencia artificial, especialmente cuando perfiles, puntuaciones o clasificaciones condicionan prestaciones, procedimientos administrativos o acceso a determinados servicios públicos esenciales.

El régimen ecuatoriano permite advertir que protección de datos y debido proceso convergen cuando una decisión automatizada utiliza información personal. Rudolf y Kovač (2024) vinculan estas tecnologías con riesgos derivados de opacidad, calidad de datos y limitaciones para comprender decisiones administrativas. La LOPDP (2021) reconoce facultades para solicitar explicaciones y ejercer derechos frente a determinadas valoraciones automatizadas. Estas garantías adquieren eficacia cuando existen procedimientos accesibles, autoridades responsables y respuestas comprensibles para la persona interesada en cada caso.

La seguridad jurídica también resulta comprometida cuando algoritmos modifican criterios decisorios sin suficiente trazabilidad. El artículo 82 de la Constitución de la República del Ecuador (2008) fundamenta este derecho en normas previas, claras, públicas y aplicadas por autoridades competentes. Un sistema automatizado que opere mediante parámetros desconocidos puede debilitar previsibilidad y confianza institucional. Por ello, las entidades públicas necesitan documentar reglas, versiones, fuentes de datos y modificaciones relevantes que intervengan en decisiones con efectos jurídicos sobre derechos ciudadanos concretos.

Figura 5

Garantías ante decisiones automatizadas



La revisión humana representa otra garantía frente a errores, sesgos o inferencias algorítmicas insuficientemente justificadas. Rudolf y Kovač (2024) señalan que la automatización administrativa debe permanecer vinculada con mecanismos de control y protección jurídica. En Ecuador, dicha revisión cobra sentido cuando permite que una autoridad competente examine datos, criterios y consecuencias antes de confirmar una decisión

controvertida. La intervención humana debe ser sustantiva, no ceremonial, pues revisar implica contar con capacidad jurídica y técnica para modificar el resultado producido.

La incorporación de decisiones automatizadas en la administración ecuatoriana requiere preservar una idea elemental: la eficiencia tecnológica carece de legitimidad cuando reduce garantías jurídicas. Constitución, Código Orgánico Administrativo y LOPDP conforman un marco que exige motivación, previsibilidad, protección de datos, contradicción y revisión efectiva. Rudolf y Kovač (2024) recuerdan que automatizar decisiones administrativas transforma relaciones entre tecnología y legalidad. El reto ecuatoriano consiste en hacer explicable el poder algorítmico y mantenerlo sometido al derecho público democrático.

2.3. Sesgos algorítmicos, discriminación digital e igualdad constitucional

Los sesgos algorítmicos introducen una preocupación jurídica cuando sistemas automatizados reproducen diferencias injustificadas entre personas o grupos. Su apariencia matemática puede transmitir neutralidad, aunque los resultados dependen de datos, variables y criterios definidos previamente. Kelly-Lyth (2023) advierte que la discriminación algorítmica puede operar mediante mecanismos menos visibles que las prácticas discriminatorias tradicionales. En Ecuador, esta cuestión compromete directamente el principio constitucional de igualdad y exige examinar los efectos materiales derivados del uso de inteligencia artificial.

La Constitución de la República del Ecuador reconoce que todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades, prohibiendo discriminaciones fundadas en categorías expresamente protegidas (Constitución de la República del Ecuador, 2008, art. 11). Esta garantía adquiere una dimensión tecnológica cuando algoritmos clasifican candidatos,

usuarios o trabajadores. Una decisión aparentemente uniforme puede producir impactos desproporcionados sobre determinados grupos, convirtiendo la neutralidad formal del sistema en una fuente efectiva de desigualdad jurídica.

El problema no reside necesariamente en una instrucción destinada a discriminar. Kelly-Lyth (2023) explica que ciertas herramientas algorítmicas pueden generar diferencias perjudiciales mediante variables indirectas, correlaciones estadísticas o datos históricos que reflejan desigualdades preexistentes. Un sistema de contratación podría valorar antecedentes aparentemente neutrales y terminar favoreciendo perfiles asociados con grupos dominantes. Desde el derecho constitucional ecuatoriano, interesa entonces evaluar efectos, criterios empleados y posibilidades reales de impugnación ante decisiones tecnológicas que produzcan tratos diferenciados injustificados.

La Ley Orgánica de Protección de Datos Personales aporta herramientas relevantes para prevenir resultados discriminatorios derivados del tratamiento automatizado. Sus principios de juridicidad, lealtad y transparencia obligan a tratar información personal de manera legítima y comprensible para sus titulares (LOPDP, 2021, art. 10). Además, la pertinencia y minimización demandan datos adecuados y limitados a las necesidades del tratamiento. Estas exigencias permiten cuestionar bases informativas excesivas, irrelevantes o capaces de introducir patrones discriminatorios en sistemas algorítmicos.

La calidad de los datos merece particular atención porque ningún algoritmo opera en un vacío social. Registros históricos pueden contener desigualdades laborales, territoriales, económicas o educativas que terminan incorporadas al aprendizaje automatizado. Kelly-Lyth (2023) analiza esta dificultad dentro del empleo, donde sistemas de selección pueden perpetuar patrones anteriores mediante criterios aparentemente objetivos. En Ecuador, el deber de igualdad requiere evaluar datos de entrenamiento,

variables utilizadas y resultados obtenidos antes de confiar decisiones relevantes a procedimientos automatizados institucionales.

La discriminación algorítmica adquiere especial sensibilidad en las relaciones laborales. Herramientas digitales pueden intervenir durante reclutamiento, selección, evaluación de desempeño, asignación de tareas o terminación de vínculos laborales. El Código del Trabajo ecuatoriano protege la igualdad en el empleo y establece obligaciones destinadas a impedir prácticas discriminatorias (Código del Trabajo, 2005). Kelly-Lyth (2023) señala que la automatización puede dificultar la identificación del trato desigual, pues las razones quedan distribuidas entre datos, modelos, proveedores tecnológicos y decisiones empresariales internas.

La protección constitucional exige mirar más allá de la intención de quien utiliza el sistema. Una organización podría desconocer que su herramienta produce diferencias sistemáticas y, aun entonces, generar consecuencias incompatibles con la igualdad. El artículo 11 de la Constitución ecuatoriana permite abordar actos discriminatorios por sus efectos, dimensión especialmente pertinente ante tecnologías automatizadas (Constitución de la República del Ecuador, 2008). El análisis jurídico debe atender resultados verificables, grupos afectados y justificaciones ofrecidas para cada diferenciación algorítmica relevante.

Transparencia y auditoría adquieren valor preventivo frente al sesgo. La LOPDP exige que el tratamiento sea transparente y que la información proporcionada al titular resulte accesible y comprensible (LOPDP, 2021). En sistemas algorítmicos, esa obligación puede traducirse en documentación sobre fuentes de datos, criterios de clasificación y mecanismos de revisión. Kelly-Lyth (2023) destaca la dificultad de detectar discriminación cuando los procesos automatizados permanecen opacos, especialmente si

quienes padecen sus consecuencias desconocen que fueron evaluados mediante algoritmos digitales.

La igualdad constitucional también reclama mecanismos institucionales capaces de corregir diferencias injustificadas antes de que produzcan daños persistentes. Revisar periódicamente resultados algorítmicos permite detectar patrones que quizá no fueron advertidos durante el diseño inicial. En materia laboral, esta vigilancia debe acompañarse de procedimientos para reclamar y obtener revisión humana. Kelly-Lyth (2023) muestra que las estructuras tradicionales antidiscriminatorias enfrentan dificultades ante decisiones algorítmicas, debido a la complejidad probatoria y a la fragmentación de responsabilidades entre distintos actores tecnológicos.

Frente a los sesgos algorítmicos, el derecho ecuatoriano dispone de principios constitucionales, reglas de protección de datos y garantías laborales capaces de orientar respuestas jurídicas. Su efectividad dependerá de traducir igualdad, transparencia y lealtad en controles concretos sobre sistemas automatizados. La tecnología puede ampliar capacidades institucionales, pero también reproducir desigualdades bajo lenguaje estadístico. Kelly-Lyth (2023) permite advertir que combatir discriminación digital requiere examinar diseño, datos y efectos, manteniendo la dignidad humana como referencia normativa permanente.

2.4. Responsabilidad civil, administrativa y penal por daños vinculados con sistemas de inteligencia artificial

La atribución de responsabilidad por daños vinculados con inteligencia artificial enfrenta una dificultad inicial: identificar quién debe responder cuando intervienen desarrolladores, proveedores, operadores, entidades públicas y usuarios. Al-Dulaimi (2025) observa que la autonomía tecnológica altera esquemas tradicionales de imputación, especialmente cuando el resultado perjudicial no proviene enteramente de una decisión humana

inmediata. En Ecuador, las categorías civiles, administrativas y penales ofrecen respuestas diferenciadas, cuya aplicación dependerá del daño, la conducta desplegada y el vínculo causal acreditado jurídicamente.

En materia civil, el daño ocasionado mediante sistemas de inteligencia artificial puede examinarse desde las reglas generales de responsabilidad previstas por el Código Civil ecuatoriano. Quien ha cometido un delito o cuasidelito que causa daño queda obligado a indemnizar, conforme al artículo 2214 (Código Civil, 2005). La intervención algorítmica no elimina esta regla, pero complica la prueba de causalidad, culpa y participación cuando el funcionamiento tecnológico depende de múltiples decisiones distribuidas entre distintos sujetos jurídicos intervinientes.

La autonomía funcional de ciertos sistemas plantea interrogantes adicionales respecto de la imputación. Al-Dulaimi (2025) examina esta cuestión señalando que los errores tecnológicos pueden dificultar la determinación de responsabilidad cuando existe distancia entre programación, operación y resultado. Desde el derecho ecuatoriano, atribuir personalidad responsable a la inteligencia artificial carece de respaldo normativo. La respuesta debe buscarse entre quienes diseñan, implementan, controlan o aprovechan el sistema, atendiendo sus deberes jurídicos y capacidad efectiva para prevenir daños previsibles.

Cuando la inteligencia artificial es utilizada por la administración pública, la responsabilidad adquiere una dimensión distinta. El Código Orgánico Administrativo regula la responsabilidad extracontractual del Estado por daños derivados de actuaciones u omisiones administrativas (Código Orgánico Administrativo, 2017). Un algoritmo empleado para asignar beneficios, evaluar solicitudes o gestionar servicios no interrumpe el vínculo entre actividad estatal y responsabilidad. Al-Dulaimi (2025) destaca que la automatización pública exige preservar

mecanismos claros de imputación, supervisión institucional y reparación ante errores tecnológicos perjudiciales.

Figura 6
Responsabilidad jurídica por daños algorítmicos



La responsabilidad administrativa también puede recaer sobre servidores o entidades cuando el empleo de sistemas automatizados incumple deberes normativos, procedimientos o estándares sectoriales aplicables. El problema requiere distinguir entre falla tecnológica inevitable y actuación administrativa negligente, deficientemente supervisada o contraria al ordenamiento. Al-Dulaimi (2025) vincula la distribución de responsabilidad con el grado de control ejercido sobre la herramienta. En Ecuador, adquirir tecnología externa no libera a la autoridad de verificar su funcionamiento, legalidad y riesgos previsibles.

La responsabilidad penal exige mayor cautela porque descansa en principios de legalidad, culpabilidad y responsabilidad personal. El Código Orgánico Integral Penal establece que una

conducta penalmente relevante debe reunir los elementos previstos por la ley y resultar atribuible al sujeto correspondiente (COIP, 2014). Un sistema de inteligencia artificial no reemplaza la valoración del dolo o la culpa cuando esta sea jurídicamente exigible. El análisis debe dirigirse hacia las personas cuya conducta guarde conexión penalmente relevante con el resultado lesivo.

Por ello, un daño producido mediante inteligencia artificial no configura automáticamente responsabilidad penal. Será necesario determinar la conducta humana relevante, el deber infringido y el elemento subjetivo requerido por el tipo penal aplicable. Al-Dulaimi (2025) advierte que la creciente autonomía de estas tecnologías tensiona modelos jurídicos construidos alrededor de decisiones humanas identificables. El COIP (2014) obliga, sin embargo, a preservar garantías de imputación personal, evitando trasladar mecánicamente al operador cualquier resultado adverso generado por un sistema complejo.

Cuando el perjuicio deriva del tratamiento de información personal, la Ley Orgánica de Protección de Datos Personales añade un régimen especializado. La LOPDP reconoce el derecho a indemnización por daños y perjuicios derivados de infracciones a sus disposiciones (LOPDP, 2021). Un modelo automatizado alimentado con datos obtenidos ilícitamente, inexactos o tratados sin observar principios legales puede generar consecuencias patrimoniales y extrapatrimoniales. La responsabilidad deberá examinar funciones, decisiones y obligaciones asumidas por responsables y encargados del tratamiento respectivo.

La distribución de responsabilidad requiere atender también la normativa sectorial aplicable. Un sistema utilizado en salud, finanzas, transporte o servicios públicos opera dentro de obligaciones profesionales y regulatorias específicas que pueden modificar el estándar de diligencia exigible. Al-Dulaimi (2025) plantea que la asignación jurídica debe considerar el control efectivo y las funciones desempeñadas por cada participante. En

Ecuador, esta lectura permite evitar respuestas uniformes y examinar deberes concretos de desarrolladores, proveedores, operadores, profesionales y autoridades competentes involucradas.

La inteligencia artificial no crea un espacio libre de responsabilidad, aunque obliga a reconsiderar criterios tradicionales de imputación y prueba. El ordenamiento ecuatoriano ofrece vías civiles, administrativas, penales y de protección de datos para responder ante daños jurídicamente relevantes. Su aplicación exige reconstruir decisiones, identificar deberes y establecer nexos causales verificables. Al-Dulaimi (2025) enfatiza la necesidad de distribuir responsabilidad conforme al control y participación efectiva, evitando que la autonomía tecnológica termine convertida en una zona de irresponsabilidad jurídica.

2.5. Inteligencia artificial generativa, autoría y titularidad de contenidos sintéticos

La inteligencia artificial generativa altera categorías tradicionales del derecho de autor al producir textos, imágenes, música y otras expresiones mediante procesos computacionales entrenados con grandes conjuntos de datos. La pregunta jurídica aparece pronto: quién puede considerarse autor cuando una persona formula instrucciones y el sistema genera el contenido. Neubauer et al. (2026) vinculan la protección autoral con la originalidad humana, criterio que obliga a distinguir entre creación intelectual personal y producción derivada predominantemente del procesamiento algorítmico automatizado.

En Ecuador, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación estructura la autoría alrededor de la persona natural. El Código Ingenios establece que únicamente la persona natural puede ser autora, mientras las personas jurídicas pueden ostentar derechos patrimoniales sobre una obra (Código Ingenios, 2016). Esta premisa adquiere especial relevancia ante contenidos sintéticos, pues un sistema generativo

carece de personalidad humana y, por tanto, no puede ocupar jurídicamente la posición originaria reservada al autor.

La dificultad aumenta cuando existe intervención humana relevante durante el proceso creativo. Una persona puede seleccionar materiales, elaborar instrucciones sucesivas, descartar resultados, modificar fragmentos y organizar el producto obtenido hasta conferirle una configuración propia. Neubauer et al. (2026) sostienen que la originalidad humana continúa siendo determinante para examinar pretensiones de autoría frente a producciones generativas. La cuestión jurídica consiste en establecer cuándo esas decisiones expresan creatividad personal suficiente para proteger el resultado bajo derechos de autor.

No toda instrucción dirigida a un modelo generativo posee necesariamente densidad creativa suficiente para fundamentar autoría sobre el resultado. Quintais (2025) examina la distancia existente entre la participación del usuario y el grado de control ejercido sobre contenidos producidos mediante inteligencia artificial generativa. Desde el régimen ecuatoriano, esta distinción resulta pertinente porque el Código Ingenios (2016) protege obras derivadas del ingenio humano. La mera solicitud funcional puede resultar insuficiente frente al requisito de creación intelectual.

La titularidad patrimonial presenta cuestiones distintas de la autoría. Aunque la calidad de autor corresponde a una persona natural, los derechos económicos pueden transferirse o atribuirse conforme a las reglas previstas por el ordenamiento. El Código Ingenios (2016) regula facultades patrimoniales y mecanismos de transmisión, mientras los contratos pueden distribuir derechos entre creadores, empresas y otros participantes. Ante herramientas generativas, conviene diferenciar autoría originaria, titularidad económica y licencias contractuales sobre contenidos producidos mediante plataformas tecnológicas determinadas.

Los términos contractuales de proveedores de inteligencia artificial adquieren relevancia cuando regulan usos permitidos, atribución de resultados, licencias y responsabilidades entre las partes. Sin embargo, un contrato no puede crear autoría allí donde el ordenamiento exige cualidades jurídicas ausentes. Neubauer et al. (2026) recuerdan que atribuir derechos sobre producciones algorítmicas requiere examinar primero la presencia de originalidad humana. En Ecuador, la autonomía contractual opera dentro de límites legales y no reemplaza los presupuestos del derecho autoral vigente.

Otra cuestión aparece cuando los modelos generativos producen contenidos cercanos a obras preexistentes. Quintais (2025) analiza las tensiones entre generación automatizada y derechos exclusivos, particularmente respecto del entrenamiento y las salidas producidas por sistemas generativos. Para el derecho ecuatoriano, una creación sintética debe examinarse atendiendo a las facultades reconocidas por el Código Ingenios (2016). La novedad tecnológica no elimina derechos anteriores ni autoriza reproducciones, transformaciones o usos sometidos a las reglas legales correspondientes vigentes.

La incertidumbre también alcanza las obras híbridas, donde aportes humanos y componentes generados mediante inteligencia artificial aparecen profundamente entrelazados. Neubauer et al. (2026) consideran que el análisis de originalidad debe concentrarse en la contribución humana identificable, evitando atribuir protección autoral al funcionamiento autónomo de la máquina. Esta perspectiva permite separar elementos protegibles de aquellos producidos algorítmicamente. En Ecuador, dicha distinción podría orientar controversias sobre textos, diseños, audiovisuales y composiciones desarrolladas mediante procesos creativos parcialmente automatizados contemporáneos.

La atribución transparente del proceso creativo puede adquirir creciente importancia probatoria. Conservar

instrucciones, versiones intermedias, ediciones y decisiones humanas permite reconstruir la participación intelectual cuando exista una controversia sobre autoría. Quintais (2025) muestra que la IA generativa obliga a revisar relaciones entre producción tecnológica y categorías del copyright. Bajo el Código Ingenios (2016), documentar aportes personales puede facilitar la identificación del creador y distinguir su actividad intelectual de resultados obtenidos principalmente mediante operaciones computacionales ejecutadas por modelos generativos.

La inteligencia artificial generativa obliga al derecho ecuatoriano a preservar una distinción esencial entre herramienta y autor. El Código Ingenios ofrece un punto de partida al reservar la autoría a personas naturales, mientras contratos y reglas patrimoniales ordenan intereses económicos derivados. Neubauer et al. (2026) sitúan la originalidad humana en el centro del debate; Quintais (2025), por su parte, evidencia tensiones regulatorias asociadas con generación automatizada. La respuesta jurídica deberá valorar siempre la contribución creativa humana comprobable.

2.6. Inteligencia artificial en la función pública: automatización administrativa, motivación y control judicial

La incorporación de inteligencia artificial en la función pública modifica prácticas administrativas vinculadas con clasificación, evaluación y resolución de asuntos ciudadanos. Estos sistemas prometen rapidez y consistencia, pero también desplazan parte del razonamiento hacia estructuras técnicas menos visibles. Ameen (2026) examina la revisión judicial de sistemas administrativos algorítmicos desde legalidad, equidad y rendición de cuentas. En Ecuador, cualquier automatización pública permanece sometida a la Constitución y al régimen jurídico que limita el ejercicio del poder estatal.

La Constitución ecuatoriana exige que las instituciones públicas ejerzan únicamente competencias atribuidas por la Constitución y la ley, conforme dispone su artículo 226 (Constitución de la República del Ecuador, 2008). Esta regla conserva plena vigencia cuando intervienen algoritmos. La administración no puede transferir su competencia jurídica a una herramienta tecnológica ni convertir el resultado computacional en autoridad autónoma. Automatizar una tarea representa una modalidad instrumental de gestión, mientras la responsabilidad decisoria permanece vinculada al órgano público competente legalmente.

La motivación constituye una garantía especialmente sensible ante actos administrativos apoyados en inteligencia artificial. El artículo 76 de la Constitución exige expresar las normas y explicar la pertinencia de su aplicación respecto de los hechos (Constitución de la República del Ecuador, 2008). Ameen (2026) vincula la revisión algorítmica con exigencias de transparencia y control efectivo. Una decisión pública no queda motivada mediante la presentación de un puntaje, clasificación o recomendación producida por un modelo computacional opaco.

El Código Orgánico Administrativo refuerza esta exigencia al regular la motivación del acto administrativo y exigir relación entre normas, hechos relevantes y régimen jurídico aplicado (Código Orgánico Administrativo, 2017). Cuando un algoritmo participa en la decisión, la autoridad necesita reconstruir los elementos que determinaron el resultado. Esto comprende datos relevantes, criterios decisorios y razones jurídicas. La complejidad técnica no puede convertirse en argumento para disminuir el deber estatal de ofrecer explicaciones comprensibles al administrado afectado directamente.

La automatización administrativa también involucra protección de datos personales cuando los sistemas procesan información identificable para clasificar ciudadanos, establecer

perfiles o recomendar decisiones. La LOPDP (2021) reconoce derechos vinculados con valoraciones automatizadas y establece principios que disciplinan el tratamiento de información personal. La administración debe verificar legitimidad, pertinencia, transparencia y seguridad del procesamiento. Ameen (2026) advierte que la rendición de cuentas algorítmica requiere mecanismos capaces de identificar responsabilidades, especialmente ante sistemas complejos utilizados por autoridades públicas.

El control judicial representa una garantía frente a decisiones administrativas tecnológicamente mediadas. Que un algoritmo participe en la formación del acto no reduce la competencia judicial para examinar legalidad, motivación y respeto de derechos. Ameen (2026) plantea que la revisión efectiva requiere acceso suficiente al funcionamiento relevante del sistema. En Ecuador, el Código Orgánico General de Procesos (2015) proporciona reglas procesales aplicables a controversias contencioso-administrativas, permitiendo someter actuaciones públicas al conocimiento de los órganos jurisdiccionales competentes.

La revisión judicial de una decisión algorítmica puede requerir elementos probatorios distintos de aquellos utilizados tradicionalmente. Documentación técnica, registros de funcionamiento, versiones del modelo y fuentes de datos pueden resultar relevantes para determinar la formación del acto impugnado. Ameen (2026) destaca la importancia de evitar que la opacidad tecnológica debilite el escrutinio judicial. El COGEP (2015), dentro de sus reglas probatorias y procesales, ofrece instrumentos que deben interpretarse atendiendo a las particularidades de actuaciones administrativas digitalizadas contemporáneas.

La Ley Orgánica para la Transformación Digital y Audiovisual impulsa la transformación digital del Estado y el

fortalecimiento de servicios públicos mediante tecnologías digitales (Asamblea Nacional del Ecuador, 2023). Ese mandato modernizador debe armonizarse con garantías constitucionales y administrativas. La eficiencia no reemplaza legalidad, motivación ni control. Cuando una institución adopta inteligencia artificial, necesita establecer responsabilidades internas, documentación y procedimientos de supervisión que permitan comprender cada decisión relevante y corregir oportunamente errores que afecten derechos ciudadanos protegidos jurídicamente.

Un problema particularmente delicado aparece cuando la administración contrata sistemas desarrollados por proveedores privados. Secretos empresariales, restricciones contractuales o arquitecturas cerradas no deberían impedir que la autoridad explique decisiones ni que un juez examine su legalidad. Ameen (2026) relaciona la responsabilidad algorítmica con posibilidades efectivas de escrutinio. En Ecuador, las entidades públicas deben prever condiciones contractuales que aseguren acceso a información necesaria para auditoría, motivación, defensa administrativa y control jurisdiccional cuando la tecnología intervenga en decisiones públicas.

La inteligencia artificial puede mejorar capacidades administrativas, pero su legitimidad depende de permanecer jurídicamente controlable. Constitución, Código Orgánico Administrativo, COGEP, LOPDP y Ley Orgánica para la Transformación Digital y Audiovisual conforman un marco desde el cual evaluar automatización pública. Ameen (2026) sitúa legalidad, equidad y rendición de cuentas entre los ejes del control judicial algorítmico. Para Ecuador, la transformación digital será compatible con el Estado de derecho cuando cada decisión automatizada pueda explicarse, revisarse y corregirse.

Tabla 2

Dimensiones jurídicas de la inteligencia artificial y mecanismos de tutela en el ordenamiento ecuatoriano

Dimensión jurídica	Implicaciones para el ordenamiento jurídico ecuatoriano
Capacidad regulatoria frente a la inteligencia artificial	Exige coordinación institucional, adaptación normativa y mecanismos de gobernanza capaces de responder al desarrollo tecnológico, articulando la Ley Orgánica para la Transformación Digital y Audiovisual con instrumentos nacionales de política pública sobre inteligencia artificial.
Decisiones automatizadas y explicabilidad	La utilización de algoritmos en decisiones con efectos jurídicos debe preservar motivación, transparencia, contradicción y revisión humana, en concordancia con la Constitución, el Código Orgánico Administrativo y la LOPDP.
Sesgos algorítmicos y discriminación digital	Los sistemas automatizados deben prevenir tratamientos diferenciados injustificados derivados de datos, variables indirectas o patrones históricos, atendiendo al principio constitucional de igualdad y a las garantías establecidas por la LOPDP.
Responsabilidad por daños algorítmicos	La imputación requiere identificar el grado de participación, control, diligencia y relación causal atribuible a desarrolladores, proveedores, operadores, entidades públicas u otros intervinientes, según corresponda a los regímenes civil, administrativo, penal o de protección de datos.
IA generativa, autoría y titularidad	La protección de contenidos sintéticos requiere distinguir la contribución creativa humana de la producción algorítmica, considerando la autoría de personas naturales, los derechos patrimoniales y las relaciones contractuales conforme al Código Ingenios.
Automatización en la función pública	La incorporación de inteligencia artificial en procedimientos administrativos permanece sometida a competencia, legalidad, motivación, protección de datos y control judicial, sin que la complejidad técnica pueda impedir la revisión efectiva de las actuaciones públicas.

Dimensión jurídica	Implicaciones para el ordenamiento jurídico ecuatoriano
Control y rendición de cuentas	La trazabilidad, documentación, auditoría, supervisión humana y posibilidad de impugnación permiten mantener los sistemas algorítmicos sujetos al derecho y facilitan la identificación de responsabilidades cuando una decisión tecnológica afecta derechos.

Nota. La tabla organiza las dimensiones desarrolladas en el Capítulo 2 a partir de Zaidan y Ibrahim (2024), Rudolf y Kovač (2024), Kelly-Lyth (2023), Al-Dulaimi (2025), Neubauer et al. (2026), Quintais (2025) y Ameen (2026), en relación con la normativa ecuatoriana examinada.

Capítulo 3:

Protección de datos personales y gobernanza jurídica de la información

La vida digital contemporánea ha convertido los datos personales en una materia cotidiana y, al mismo tiempo, profundamente jurídica. Cada registro, búsqueda, transacción o identificación puede alimentar estructuras capaces de clasificar personas y orientar decisiones. En Ecuador, esta realidad exige leer la protección de datos como un derecho con autonomía normativa y capacidad para limitar poderes informacionales. Izquierdo-Rodas (2026) vincula esta protección con salvaguardas destinadas a responder ante riesgos tecnológicos y vulneraciones propias de entornos digitalizados.

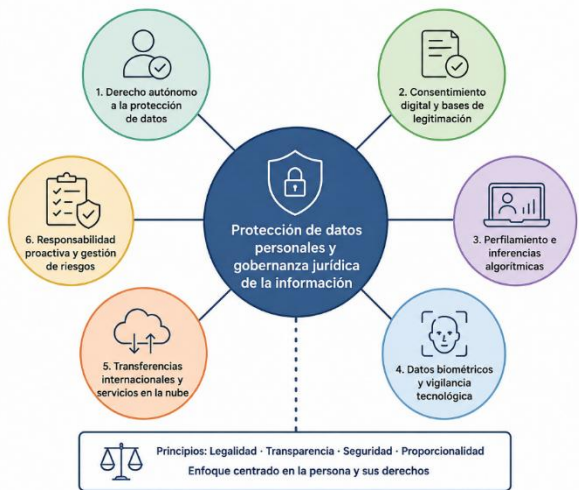
El reconocimiento jurídico del dato personal cambia la relación entre individuo, tecnología e instituciones. Ya no interesa únicamente preservar una esfera íntima frente a intromisiones, pues también importa conservar facultades de decisión sobre información que circula legítimamente. Izquierdo-Rodas (2026) destaca que protección de datos y ciberseguridad mantienen vínculos estrechos ante riesgos derivados de la transformación tecnológica. Desde esa perspectiva, la legislación ecuatoriana construye garantías que acompañan a la información durante las distintas operaciones que integran su tratamiento.

Una primera cuestión aparece con el consentimiento digital. Pulsar una casilla puede parecer un gesto menor, aunque detrás de esa acción existen condiciones jurídicas destinadas a preservar libertad e información suficiente. Santos et al. (2021) muestran que las plataformas de gestión del consentimiento pueden desempeñar funciones diversas dentro de las operaciones de tratamiento, haciendo necesario delimitar responsabilidades. El problema adquiere mayor densidad cuando enormes cantidades de información circulan entre actores tecnológicos cuyas intervenciones permanecen poco visibles para las personas.

La capacidad de procesar información también permite inferir aquello que una persona nunca declaró expresamente. Preferencias, probabilidades, afinidades o riesgos pueden

construirse mediante relaciones estadísticas entre individuos. Mühlhoff (2024) advierte que la analítica predictiva posee una dimensión colectiva, dado que los datos de ciertos sujetos permiten formular predicciones acerca de otros. Esta característica obliga a ampliar la mirada jurídica sobre perfilamiento y automatización, especialmente cuando una inferencia condiciona oportunidades, servicios o decisiones relevantes para la vida individual.

Figura 7
Gobernanza jurídica de los datos personales



La intensidad del tratamiento aumenta cuando el propio cuerpo se transforma en identificador. Rostro, huellas, voz y otros atributos biométricos pueden facilitar procesos de autenticación, pero también permiten desarrollar mecanismos persistentes de identificación y vigilancia. Hogenhout y Wangmo (2025) examinan la privacidad facial desde una perspectiva comparada y destacan la necesidad de garantías específicas frente al procesamiento biométrico. La discusión alcanza una dimensión especialmente sensible cuando estas tecnologías funcionan a distancia y sin participación consciente del individuo observado.

Los datos tampoco permanecen necesariamente dentro de las fronteras ecuatorianas. Servicios digitales y arquitecturas de nube distribuyen almacenamiento y procesamiento entre infraestructuras ubicadas en diversas jurisdicciones. García Cáceres (2025) relaciona esta configuración tecnológica con cuestiones de soberanía digital y derecho internacional, donde control, jurisdicción y dependencia tecnológica adquieren especial relevancia. En consecuencia, proteger información personal requiere atender su movilidad transfronteriza y las condiciones jurídicas que deben acompañarla cuando proveedores internacionales intervienen en operaciones desarrolladas para organizaciones ecuatorianas.

La gobernanza jurídica de la información exige, además, abandonar una visión meramente reactiva del cumplimiento. Esperar una vulneración para adoptar medidas resulta incompatible con tratamientos capaces de producir efectos amplios y difíciles de revertir. Friedewald et al. (2021) explican que las evaluaciones de impacto permiten trasladar principios de protección hacia prácticas organizacionales orientadas a identificar riesgos anticipadamente. Prevenir adquiere entonces un sentido jurídico concreto: examinar tratamientos, documentar decisiones y establecer medidas proporcionadas antes de comprometer derechos personales.

Esta perspectiva preventiva adquiere una dimensión adicional cuando intervienen sistemas algorítmicos. Una evaluación técnicamente correcta puede resultar insuficiente si no considera efectos diferenciados entre personas o grupos. Kasirzadeh y Clifford (2021) vinculan las evaluaciones de impacto con cuestiones de equidad, mostrando que protección de datos y justicia algorítmica mantienen puntos de encuentro relevantes. La responsabilidad proactiva requiere, por ello, una mirada capaz de conectar seguridad, proporcionalidad, diseño tecnológico y

consecuencias derivadas del uso institucional de información personal.

A través de estas materias aparece una preocupación compartida: evitar que la capacidad tecnológica determine por sí misma aquello que resulta jurídicamente admisible. Santos et al. (2021) evidencian esta tensión al estudiar responsabilidades dentro de infraestructuras de consentimiento, mientras Mühlhoff (2024) la proyecta hacia inferencias construidas mediante relaciones colectivas. Desde otra vertiente, García Cáceres (2025) la sitúa ante infraestructuras globales de nube. Son escenarios distintos, pero convergen alrededor del poder asociado al tratamiento de información.

Este capítulo aborda, por tanto, la protección de datos como una arquitectura jurídica que conecta autonomía personal, legitimación, transparencia, perfilamiento, biometría, transferencias internacionales y responsabilidad preventiva. Hogenhout y Wangmo (2025) permiten advertir la intensidad de los riesgos biométricos, mientras Kasirzadeh y Clifford (2021) recuerdan la importancia de examinar efectos distributivos. En Ecuador, estas discusiones adquieren especial significado frente a una transformación digital que reclama innovación, pero también límites verificables, responsabilidades institucionales y garantías efectivas para las personas.

3.1. La protección de datos personales como derecho autónomo en el sistema jurídico ecuatoriano

En el sistema jurídico ecuatoriano, la protección de datos personales posee identidad y no puede reducirse a una extensión de la intimidad. La Constitución reconoce facultades específicas sobre la información personal, entre ellas acceso, decisión y resguardo, dentro del catálogo de derechos de libertad (Constitución de la República del Ecuador, 2008, art. 66). Esta formulación constitucional permite comprender que la persona mantiene poder

jurídico sobre datos capaces de describirla, identificarla o afectar su esfera individual.

La autonomía de este derecho adquiere precisión con la Ley Orgánica de Protección de Datos Personales, cuyo propósito es garantizar el acceso efectivo, decisión y protección jurídica respecto de sus datos. La norma convierte la autodeterminación informativa en una posición jurídica exigible frente a responsables y encargados del tratamiento. Desde esta perspectiva, Izquierdo-Rodas (2026) vincula la regulación de datos con garantías destinadas a reducir riesgos derivados del uso tecnológico de información personal en entornos digitales.

La diferencia entre intimidad y protección de datos resulta relevante porque una información personal no necesita pertenecer a la vida privada para recibir tutela jurídica. Un nombre, una dirección o un identificador pueden circular legítimamente y, pese a ello, permanecer sometidos a reglas de tratamiento. El artículo 66 de la Constitución ecuatoriana reconoce esta capacidad de decisión, mientras la LOPDP desarrolla condiciones para recolectar, utilizar, conservar y transferir información dentro de límites verificables y exigibles.

Esta configuración transforma a la persona en titular de facultades frente al tratamiento de información que le concierne. La LOPDP reconoce derechos de acceso, rectificación, eliminación, oposición y otras potestades que permiten intervenir en distintas etapas del tratamiento. No se trata de una declaración abstracta, sino de mecanismos destinados a equilibrar relaciones marcadas por desigualdades informativas. Izquierdo-Rodas (2026) advierte que la expansión tecnológica incrementa riesgos vinculados con exposición, uso indebido y vulneraciones de datos personales.

El carácter autónomo también se aprecia en los principios que ordenan el tratamiento. La LOPDP exige juridicidad, lealtad, transparencia, pertinencia, minimización, proporcionalidad,

conservación limitada, seguridad y responsabilidad, entre otros criterios que disciplinan decisiones institucionales. Estas reglas trasladan la protección desde una reacción posterior al daño hacia deberes de prevención. El Reglamento General a la LOPDP complementa esa arquitectura mediante disposiciones operativas que orientan la aplicación de obligaciones, garantías y procedimientos previstos por la legislación ecuatoriana.

Desde una mirada, la autonomía no implica aislamiento frente a otros derechos. La protección de datos dialoga con intimidad, honra, identidad, igualdad y libertad, pero conserva un objeto específico: el control jurídico de la información personal durante su tratamiento. Esa relación explica por qué una afectación informativa puede comprometer derechos simultáneamente. La Constitución ecuatoriana, en su artículo 66, ofrece el fundamento superior, mientras la LOPDP establece un régimen especializado para materializar facultades, deberes y garantías.

La dimensión institucional refuerza esta lectura. Un derecho autónomo requiere vías de tutela, autoridades y obligaciones capaces de producir consecuencias ante tratamientos contrarios al ordenamiento. La LOPDP organiza responsabilidades para quienes determinan o ejecutan operaciones sobre datos, mientras su Reglamento General precisa aspectos para el cumplimiento. Esta estructura responde a una realidad señalada por Izquierdo-Rodas (2026): la digitalización amplía oportunidades, pero también intensifica riesgos de seguridad, exposición y utilización ilegítima de información vinculada con personas.

La autonomía adquiere sentido ante sistemas automatizados, plataformas digitales y bases de datos capaces de relacionar información procedente de fuentes. En estas dinámicas, el daño no depende de revelar un secreto; puede originarse en perfiles inexactos, decisiones discriminatorias, conservación excesiva o tratamientos incompatibles con el propósito informado.

La LOPDP proporciona criterios para examinar tales prácticas desde los derechos del titular. Izquierdo-Rodas (2026) destaca la necesidad de salvaguardas frente a riesgos tecnológicos en la era digital.

Existe una dimensión democrática en este reconocimiento. Cuando las personas conocen qué datos se tratan, para qué propósito y bajo qué fundamento, pueden ejercer derechos y cuestionar decisiones que afecten su vida. La transparencia deja de ser cortesía organizacional y se convierte en obligación jurídica. La LOPDP y su Reglamento articulan deberes para hacer comprensible el tratamiento, mientras la Constitución preserva la decisión sobre información personal (Constitución de la República del Ecuador, 2008, art. 66).

En Ecuador, reconocer la protección de datos personales como derecho autónomo permite ordenar jurídicamente una sociedad en que la información circula con velocidad y adquiere valor económico y político. La Constitución aporta la base de control personal; la LOPDP desarrolla derechos, principios y obligaciones; su Reglamento General facilita su aplicación. Izquierdo-Rodas (2026) relaciona protección de datos y ciberseguridad con respuestas orientadas a contener riesgos. La autonomía expresa una garantía de dignidad frente al poder informacional.

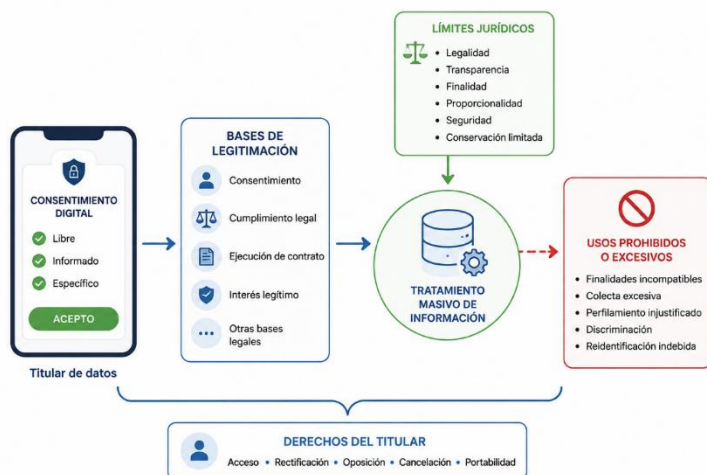
3.2. Consentimiento digital, bases de legitimación y límites jurídicos al tratamiento masivo de información

El consentimiento digital ocupa un lugar relevante dentro del régimen ecuatoriano de protección de datos, aunque no constituye la única base jurídica capaz de legitimar el tratamiento. La Ley Orgánica de Protección de Datos Personales exige que la manifestación del titular reúna condiciones que permitan reconocer una voluntad libre, específica, informada e inequívoca (LOPDP, 2021). En entornos digitales, estas exigencias adquieren

especial importancia debido a interfaces que pueden orientar decisiones mediante diseños poco transparentes.

Figura 8

Consentimiento y legitimación del tratamiento de datos



La validez del consentimiento depende de una decisión auténtica y comprensible, no de una aceptación meramente formal obtenida mediante casillas, avisos extensos o mecanismos configurados para favorecer determinada respuesta. Santos et al. (2021) examinan las plataformas de gestión de consentimiento y muestran que su participación puede generar interrogantes acerca de responsabilidades jurídicas durante el tratamiento. Esta cuestión resulta pertinente cuando varios actores tecnológicos intervienen en la recopilación, transmisión y administración de preferencias del usuario digital.

La LOPDP establece diversas bases de legitimación que permiten tratar datos personales cuando existe fundamento jurídico suficiente. El consentimiento representa una de ellas, junto con otras circunstancias reconocidas legalmente para atender

obligaciones, relaciones jurídicas o intereses protegidos por el ordenamiento (LODPD, 2021). Esta pluralidad evita convertir toda operación informativa en dependiente de una autorización individual. Sin embargo, quien realiza el tratamiento debe identificar previamente la base aplicable y acreditar que concurren sus presupuestos jurídicos correspondientes.

El tratamiento masivo plantea tensiones particulares porque la acumulación de información permite establecer perfiles, inferir comportamientos y relacionar registros procedentes de múltiples fuentes. La existencia de grandes volúmenes de datos no elimina las exigencias de legitimidad, transparencia y proporcionalidad previstas por la LODPD. Cada operación requiere fundamento jurídico y propósito determinado. En esta materia, la capacidad tecnológica para procesar información a gran escala no equivale, por sí misma, a una autorización normativa para utilizarla indiscriminadamente.

La transparencia constituye una garantía estrechamente vinculada con la legitimación del tratamiento. El titular necesita recibir información comprensible acerca de las operaciones realizadas, sus propósitos y los sujetos que intervienen en ellas. El Reglamento General a la LODPD desarrolla disposiciones destinadas a hacer efectivas las obligaciones de información dentro de las relaciones digitales. Santos et al. (2021) destacan que las estructuras técnicas de consentimiento pueden involucrar diferentes participantes, circunstancia que vuelve relevante delimitar responsabilidades entre ellos.

El deber de información adquiere especial importancia cuando las prácticas digitales presentan cadenas extensas de tratamiento. Una persona puede entregar datos a una plataforma sin advertir que posteriormente intervienen proveedores tecnológicos, intermediarios publicitarios u otros participantes. Frente a esta realidad, la LODPD exige transparencia respecto del tratamiento y reconoce facultades al titular para ejercer control

sobre su información. La legitimidad jurídica requiere, entonces, que las operaciones sean explicables y compatibles con los propósitos previamente comunicados al interesado.

Las plataformas de gestión de consentimiento permiten observar que una herramienta diseñada para registrar preferencias también puede intervenir activamente en decisiones relacionadas con datos personales. Santos et al. (2021) analizan esta cuestión desde la distribución de responsabilidades entre controladores y procesadores, destacando que la calificación jurídica depende de las funciones efectivamente desarrolladas. Esta perspectiva resulta útil para Ecuador, donde la LOPDP atribuye obligaciones según la posición que cada participante ocupa durante las operaciones de tratamiento de datos.

Los límites jurídicos adquieren mayor relevancia cuando el tratamiento masivo persigue propósitos comerciales, analíticos o predictivos. La disponibilidad técnica de información no libera al responsable de justificar su utilización mediante una base legítima. Tampoco una autorización amplia debería interpretarse como permiso indefinido para efectuar operaciones distintas de aquellas conocidas por el titular. La LOPDP vincula el tratamiento con principios que restringen usos incompatibles, mientras su Reglamento General aporta criterios para materializar deberes de transparencia e información.

En las relaciones digitales existe una distancia frecuente entre pulsar una opción y comprender las consecuencias jurídicas asociadas. Esa diferencia obliga a valorar el consentimiento atendiendo a la calidad de la información proporcionada y a las condiciones en que fue obtenido. Santos et al. (2021) evidencian que los mecanismos tecnológicos de gestión pueden involucrar estructuras complejas de responsabilidad. Para el derecho ecuatoriano, esta observación permite insistir en que la arquitectura tecnológica debe respetar las garantías previstas por la LOPDP.

La gobernanza jurídica de información requiere superar la idea de que una aceptación digital legitima cualquier tratamiento posterior. Consentimiento, transparencia, deber de información y demás bases previstas por la LOPDP conforman un sistema destinado a limitar el poder derivado de la acumulación de datos. El Reglamento General refuerza su aplicación mediante reglas operativas. En diálogo con Santos et al. (2021), esta arquitectura permite examinar responsabilidades y preservar capacidad decisoria de las personas frente a tratamientos masivos contemporáneos.

3.3. Perfilamiento, inferencias algorítmicas y tratamiento automatizado de datos personales

El perfilamiento transforma datos dispersos en representaciones capaces de orientar decisiones sobre personas concretas. En Ecuador, esta práctica queda sometida a la Ley Orgánica de Protección de Datos Personales cuando emplea información vinculada con individuos identificados o identificables. Su relevancia jurídica aumenta cuando modelos estadísticos atribuyen preferencias, capacidades o riesgos. Mühlhoff (2024) advierte que la analítica predictiva amplía la protección hacia inferencias que afectan también a grupos cuyos integrantes pueden no haber aportado datos directamente.

Las inferencias algorítmicas plantean una cuestión jurídica distinta de la mera recolección de información. Un sistema puede deducir rasgos, intereses o probabilidades que nunca fueron declarados por el titular. Mühlhoff (2024) examina esta capacidad predictiva y destaca sus efectos colectivos, pues determinadas categorías se construyen mediante patrones compartidos. La LOPDP exige que el tratamiento respete principios de juridicidad, transparencia, pertinencia y proporcionalidad, exigencias aplicables cuando una inferencia adquiere relevancia para una persona determinada en Ecuador.

El tratamiento automatizado adquiere especial sensibilidad cuando produce decisiones con efectos jurídicos o repercusiones significativas para el titular. La LOPDP reconoce derechos vinculados con estas operaciones y permite cuestionar decisiones sustentadas en valoraciones automatizadas bajo los presupuestos establecidos. El Reglamento General desarrolla elementos para el ejercicio de tales garantías. Esta regulación procura impedir que la eficiencia computacional desplace la posibilidad humana de comprender, objetar o solicitar revisión frente a resultados que inciden sobre derechos personales.

Una característica inquietante del perfilamiento reside en su aparente distancia respecto de la persona observada. Los modelos trabajan con correlaciones, agrupaciones y probabilidades; pese a ello, sus resultados pueden condicionar oportunidades. Mühlhoff (2024) sostiene que la analítica predictiva opera mediante relaciones colectivas entre datos, donde información de unas personas permite formular predicciones sobre otras. Esta dinámica obliga a interpretar la protección jurídica más allá del dato entregado, atendiendo también a conocimientos derivados mediante procesamiento algorítmico.

La transparencia adquiere un significado ante sistemas capaces de generar inferencias difíciles de advertir desde fuera. Informar acerca de la recolección resulta insuficiente cuando el tratamiento persigue clasificar, predecir o evaluar conductas. La LOPDP reconoce al titular facultades relacionadas con información y decisiones automatizadas, mientras el Reglamento General precisa su aplicación. Desde la perspectiva de Mühlhoff (2024), comprender la dimensión colectiva de las predicciones permite advertir que la afectación puede extenderse entre individuos vinculados estadísticamente.

El problema jurídico no radica en que una predicción sea incorrecta. Una inferencia estadísticamente acertada también puede producir consecuencias injustificadas cuando se emplea

fuera de límites legítimos o con efectos desproporcionados. La LOPDP exige observar principios y derechos durante todo tratamiento de datos personales. Esta exigencia alcanza prácticas de perfilamiento cuando afectan al titular. Mühlhoff (2024) aporta una mirada complementaria al señalar que las predicciones dependen de patrones contruidos mediante información proveniente de poblaciones enteras.

Los derechos del titular funcionan como contrapesos frente a la opacidad que puede acompañar al procesamiento automatizado. Acceso, oposición y demás facultades reconocidas por la LOPDP permiten intervenir jurídicamente ante usos de información personal. En materia de decisiones automatizadas, estas garantías cobran intensidad cuando una evaluación algorítmica condiciona posiciones individuales. El Reglamento General complementa su ejercicio mediante reglas de aplicación, procurando que la automatización permanezca sometida a controles jurídicos y a responsabilidades institucionales claramente identificables.

La dimensión colectiva estudiada por Mühlhoff (2024) resulta fértil para analizar sistemas predictivos contemporáneos. Quien nunca entregó determinada información puede recibir una clasificación construida mediante semejanzas con otras personas. El derecho de protección de datos enfrenta entonces una realidad donde las inferencias circulan entre categorías estadísticas y sujetos. Bajo la LOPDP, el tratamiento debe conservar fundamento jurídico y respetar derechos del titular, incluso cuando el conocimiento aplicado provenga de modelos entrenados con datos de terceros.

El perfilamiento también altera la relación entre conocimiento y poder. Una organización capaz de anticipar comportamientos dispone de ventajas que el titular puede observar o contrarrestar sin garantías jurídicas. La regulación ecuatoriana responde mediante principios, obligaciones y derechos aplicables al

tratamiento automatizado. El Reglamento General a la LOPDP contribuye a precisar mecanismos de aplicación. Mühlhoff (2024) permite añadir que el poder predictivo descansa en estructuras colectivas, por lo que sus consecuencias exceden relaciones estrictamente individuales.

La gobernanza jurídica del perfilamiento requiere reconocer que los algoritmos no producen inferencias en un vacío normativo. Cada clasificación puede involucrar legitimidad, transparencia, proporcionalidad, derechos del titular y responsabilidades de quienes determinan el tratamiento. La LOPDP y su Reglamento General ofrecen el marco para examinar estas operaciones. Mühlhoff (2024) amplía la discusión al mostrar que la predicción utiliza relaciones entre individuos y grupos, recordando que proteger datos personales exige atender efectos derivados del conocimiento estadístico.

3.4. Datos biométricos, reconocimiento facial y vigilancia tecnológica

Los datos biométricos ocupan una posición especialmente delicada dentro del derecho ecuatoriano porque permiten identificar personas mediante rasgos físicos, fisiológicos o conductuales. Rostro, huellas y patrones corporales adquieren valor informacional cuando son procesados técnicamente para autenticar o individualizar sujetos. La LOPDP los ubica entre las categorías especiales de datos personales, sometidas a protección reforzada (LOPDP, 2021). Esta calificación responde a una característica evidente: determinados atributos biométricos acompañan permanentemente a la persona durante su vida.

El reconocimiento facial lleva esta sensibilidad hacia espacios donde la identificación puede producirse a distancia, incluso sin interacción consciente del individuo. Una cámara registra imágenes; posteriormente, sistemas computacionales extraen características y comparan patrones con referencias

almacenadas. Hogenhout y Wangmo (2025) examinan la privacidad facial desde diversos modelos regulatorios y destacan la necesidad de garantías frente al procesamiento biométrico. La cuestión jurídica comienza, precisamente, cuando observar deja de significar mirar y pasa a significar identificar técnicamente.

La Constitución ecuatoriana proporciona fundamentos relevantes para examinar estas tecnologías desde la dignidad, intimidad y protección de datos personales. El artículo 66 reconoce derechos vinculados con la esfera personal y con el control sobre información referente al individuo (Constitución de la República del Ecuador, 2008, art. 66). Cuando una tecnología biométrica captura características corporales y las convierte en identificadores procesables, la intervención jurídica debe valorar tanto la legitimidad del tratamiento como sus consecuencias para libertades personales.

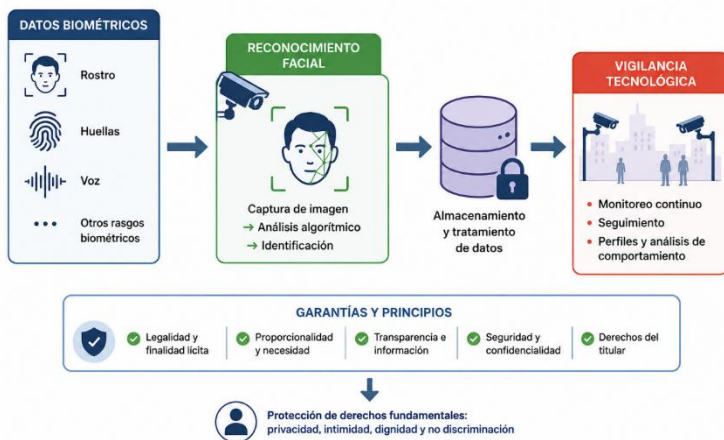
La vigilancia tecnológica intensifica estas preocupaciones cuando dispositivos biométricos operan de manera continua en calles, establecimientos, centros laborales o servicios. El problema no reside únicamente en captar imágenes, sino en convertirlas en datos capaces de ser comparados, almacenados y relacionados. Hogenhout y Wangmo (2025) muestran que la regulación biométrica comparada responde precisamente a riesgos asociados con identificación facial. En Ecuador, la LOPDP exige examinar estas operaciones mediante principios de juridicidad, transparencia, proporcionalidad y seguridad.

La naturaleza sensible del dato biométrico obliga a diferenciar entre necesidad tecnológica y mera conveniencia administrativa. Que un sistema facial facilite accesos o verificaciones no convierte automáticamente su utilización en jurídicamente admisible. La LOPDP establece un régimen reforzado para categorías especiales y exige fundamento habilitante para su tratamiento. El Reglamento General desarrolla disposiciones destinadas a concretar obligaciones de responsables

y encargados. Cada implementación biométrica demanda, por ello, una justificación compatible con los derechos del titular involucrado.

Figura 9

Biometría, reconocimiento facial y vigilancia digital



Existe además una particularidad material difícil de ignorar: ante la exposición de una contraseña, esta puede reemplazarse; frente a la vulneración de una plantilla biométrica, las posibilidades de sustitución resultan limitadas. Hogenhout y Wangmo (2025) relacionan esta permanencia con la necesidad de protección rigurosa de la privacidad facial. La legislación ecuatoriana responde mediante deberes de seguridad y responsabilidad aplicables al tratamiento, especialmente relevantes cuando los datos comprometidos permiten autenticar o identificar inequívocamente individuos.

El reconocimiento facial utilizado con fines de vigilancia puede modificar la experiencia cotidiana del espacio público. Una persona que sabe que sus movimientos pueden ser identificados,

registrados y vinculados con bases informativas enfrenta una relación distinta con el entorno. La Constitución protege intimidad y datos personales, mientras la LOPDP establece garantías frente a tratamientos que comprometan tales derechos. Hogenhout y Wangmo (2025) permiten advertir que la privacidad facial merece atención específica por sus implicaciones individuales y sociales.

La proporcionalidad ofrece un criterio especialmente valioso para evaluar sistemas biométricos. No toda finalidad legítima autoriza cualquier intensidad de tratamiento, especialmente cuando existen mecanismos menos invasivos para alcanzar resultados equivalentes. Bajo la LOPDP, el uso de información personal debe responder a principios que limitan tratamientos excesivos. El Reglamento General complementa esta disciplina mediante reglas para aplicar obligaciones y garantías. En vigilancia tecnológica, esta valoración requiere considerar alcance, duración, población afectada, almacenamiento y riesgos previsibles asociados.

También importa quién administra la infraestructura biométrica y con qué capacidad de reutilización. Bases creadas para controlar accesos podrían adquirir otros propósitos si no existen límites jurídicos efectivos. Hogenhout y Wangmo (2025) analizan distintos enfoques regulatorios que buscan restringir usos incompatibles de información facial. En Ecuador, la LOPDP vincula el tratamiento con propósitos determinados y derechos exigibles, mientras su Reglamento General contribuye a ordenar procedimientos de cumplimiento. La confianza pública depende de límites verificables institucionalmente.

La gobernanza de datos biométricos requiere reconocer que el cuerpo se ha convertido en fuente permanente de información digitalizable. Rostro, voz o huellas pueden facilitar autenticación y seguridad, pero también habilitar formas intensivas de vigilancia. La LOPDP, su Reglamento General y las garantías constitucionales ofrecen parámetros para limitar estas prácticas.

Hogenhout y Wangmo (2025) aportan una perspectiva comparada que refuerza una premisa jurídica esencial: la innovación biométrica debe permanecer subordinada a dignidad y derechos fundamentales.

3.5. Transferencias internacionales de datos, servicios en la nube y soberanía informacional

Las transferencias internacionales de datos expresan una tensión propia de la economía digital: la información atraviesa fronteras con enorme facilidad, mientras las garantías jurídicas permanecen vinculadas a ordenamientos territoriales. La LOPDP ecuatoriana regula transferencias y comunicaciones internacionales para preservar los derechos del titular cuando sus datos abandonan determinadas jurisdicciones (LOPDP, 2021). Esta protección adquiere especial relevancia ante servicios tecnológicos distribuidos globalmente, donde almacenamiento, procesamiento y respaldo pueden ejecutarse en países distintos de manera simultánea.

Los servicios en la nube profundizan esa movilidad porque separan físicamente al usuario de la infraestructura que conserva y procesa su información. Una organización ecuatoriana puede contratar recursos tecnológicos administrados desde múltiples jurisdicciones sin percibir cotidianamente esa fragmentación territorial. García Cáceres (2025) vincula esta arquitectura con interrogantes de soberanía digital y derecho internacional. Desde la perspectiva jurídica ecuatoriana, conocer la ubicación, circulación y tratamiento de datos constituye una condición relevante para gestionar responsabilidades y garantías efectivas.

La soberanía informacional no debe entenderse necesariamente como obligación de mantener todos los datos dentro del territorio nacional. Su significado jurídico puede relacionarse con la capacidad estatal de preservar derechos, ejercer competencias regulatorias y evitar que la externalización

tecnológica vacíe las garantías internas. García Cáceres (2025) analiza la soberanía digital frente a infraestructuras de nube sometidas a relaciones transnacionales. Esta perspectiva permite observar que la dependencia tecnológica también produce interrogantes sobre jurisdicción, control y autonomía regulatoria.

La LOPDP establece reglas destinadas a disciplinar las transferencias internacionales y evitar que el desplazamiento territorial de información reduzca el nivel de protección reconocido a las personas. La transferencia requiere atender las condiciones previstas por el régimen jurídico y valorar las garantías existentes en el destino o mediante mecanismos aplicables (LOPDP, 2021). El Reglamento General desarrolla esta materia con disposiciones operativas, ofreciendo criterios para que responsables y encargados documenten adecuadamente operaciones internacionales vinculadas con datos personales.

En la nube, transferir información rara vez constituye un acto aislado. Los datos pueden replicarse por razones de disponibilidad, distribuirse entre centros de procesamiento o desplazarse durante operaciones de respaldo y recuperación. Esta arquitectura vuelve indispensable conocer las cadenas contractuales que sostienen el servicio. García Cáceres (2025) relaciona las infraestructuras digitales globales con problemas de soberanía y derecho internacional. Para las organizaciones ecuatorianas, contratar capacidad tecnológica externa no elimina obligaciones derivadas de la normativa nacional.

La responsabilidad jurídica conserva importancia cuando participan proveedores establecidos fuera del Ecuador. Externalizar almacenamiento o procesamiento no significa externalizar el deber de proteger derechos. La LOPDP mantiene obligaciones relacionadas con seguridad, transparencia, legitimidad y responsabilidad durante el tratamiento de información personal. Su Reglamento General aporta instrumentos para concretar dichas exigencias. En términos prácticos, la contratación de servicios de

nube exige evaluar proveedores, condiciones contractuales, destinos internacionales y medidas capaces de mantener garantías durante cada fase del tratamiento transfronterizo.

La Ley Orgánica para la Transformación Digital y Audiovisual aporta otra dimensión al debate, pues impulsa procesos de digitalización dentro de una política normativa orientada a modernizar actividades y servicios. Esa transformación convive necesariamente con las garantías establecidas por la LOPDP. La expansión de infraestructuras digitales requiere, por tanto, coordinación entre innovación, seguridad y protección jurídica. La soberanía informacional cobra sentido cuando la modernización tecnológica mantiene capacidad institucional para proteger derechos y controlar dependencias derivadas de servicios transnacionales.

Existe también una cuestión de poder detrás de la infraestructura. Quien administra centros de datos, plataformas y recursos computacionales posee capacidades materiales que pueden condicionar decisiones públicas y privadas. García Cáceres (2025) examina la soberanía digital precisamente desde relaciones entre nube y derecho internacional. Para Ecuador, esta discusión invita a valorar dependencia tecnológica, jurisdicciones aplicables y posibilidades regulatorias. La gobernanza informacional requiere conocer no únicamente dónde están los datos, sino quién puede disponer jurídicamente de ellos.

Las transferencias internacionales exigen transparencia hacia el titular porque la circulación transfronteriza puede modificar riesgos, actores participantes y marcos jurídicos aplicables. La LOPDP y su Reglamento General establecen deberes relacionados con información y protección durante operaciones de tratamiento internacional. Este régimen busca conservar continuidad jurídica pese al movimiento de los datos. García Cáceres (2025) permite ampliar la mirada: las decisiones sobre infraestructura digital también expresan relaciones de soberanía,

autonomía tecnológica y capacidad estatal frente a proveedores globales.

La soberanía informacional ecuatoriana se construye mediante reglas capaces de acompañar los datos más allá de las fronteras, sin desconocer la naturaleza distribuida de la tecnología contemporánea. La LOPDP disciplina transferencias internacionales; su Reglamento General concreta mecanismos de aplicación, mientras la Ley Orgánica para la Transformación Digital y Audiovisual impulsa procesos de modernización. García Cáceres (2025) aporta una lectura donde nube y soberanía digital convergen, recordando que innovación tecnológica y autonomía jurídica deben permanecer articuladas.

3.6. Responsabilidad proactiva, evaluación de impacto y cumplimiento regulatorio basado en riesgos

La responsabilidad proactiva modifica la manera de comprender el cumplimiento en materia de protección de datos personales. No basta reaccionar después de una vulneración; responsables y encargados deben adoptar medidas capaces de demostrar observancia permanente de sus obligaciones. La LOPDP incorpora esta lógica mediante principios, deberes de seguridad y mecanismos preventivos aplicables al tratamiento (LOPDP, 2021). El cumplimiento adquiere entonces carácter organizacional: requiere decisiones documentadas, controles verificables y una cultura institucional orientada a prevenir afectaciones sobre derechos personales.

El enfoque basado en riesgos permite graduar medidas atendiendo a la naturaleza, alcance y posibles consecuencias de cada tratamiento. Una base administrativa ordinaria no presenta necesariamente las mismas amenazas que un sistema biométrico o una plataforma de perfilamiento. El Reglamento General a la LOPDP desarrolla obligaciones relacionadas con gestión de riesgos y medidas de protección. Friedewald et al. (2021) destacan que las

evaluaciones de impacto trasladan principios generales hacia procedimientos capaces de identificar y gestionar afectaciones previsibles.

La evaluación de impacto en protección de datos constituye una herramienta preventiva destinada a examinar tratamientos que pueden generar riesgos elevados para derechos y libertades. Su valor reside en anticipar problemas antes de consolidar decisiones técnicas difíciles de revertir. La LOPDP contempla este instrumento dentro de su arquitectura de responsabilidad proactiva. Kasirzadeh y Clifford (2021) vinculan las evaluaciones de impacto con interrogantes sobre equidad, mostrando que analizar riesgos exige atender también consecuencias distributivas derivadas del procesamiento de información personal.

Evaluar impacto no equivale a completar mecánicamente un formulario. El proceso requiere describir operaciones, identificar riesgos, valorar su gravedad y determinar medidas destinadas a reducirlos. Friedewald et al. (2021) estudian la aplicación práctica de estas evaluaciones y muestran su relevancia para convertir obligaciones jurídicas en decisiones organizacionales. En Ecuador, la LOPDP y su Reglamento General permiten integrar esta metodología dentro del cumplimiento, particularmente ante tratamientos cuya naturaleza pueda afectar intensamente los derechos de los titulares involucrados.

La protección desde el diseño refuerza esta orientación preventiva al exigir que las garantías sean consideradas durante la concepción de sistemas, productos y procedimientos. Corregir posteriormente una arquitectura invasiva puede resultar costoso e insuficiente. La LOPDP incorpora deberes relacionados con protección de datos desde el diseño y por defecto, mientras su Reglamento General desarrolla criterios de aplicación. Esta perspectiva desplaza parte del esfuerzo regulatorio hacia etapas

tempranas, donde todavía resulta posible modificar decisiones técnicas antes de generar afectaciones relevantes.

El análisis de riesgos también obliga a observar la seguridad desde una perspectiva dinámica. Las amenazas cambian, las tecnologías evolucionan y los tratamientos pueden adquirir usos diferentes con el tiempo. Por ello, medidas inicialmente adecuadas requieren revisión periódica. La LOPDP establece obligaciones de seguridad vinculadas con los riesgos del tratamiento. Friedewald et al. (2021) muestran que la evaluación de impacto funciona mejor cuando permanece conectada con procesos reales de gestión, documentación y revisión dentro de las organizaciones responsables.

La equidad aporta una dimensión adicional a las evaluaciones de impacto, especialmente cuando intervienen sistemas automatizados. Kasirzadeh y Clifford (2021) examinan las relaciones entre justicia algorítmica y protección de datos, señalando tensiones que una evaluación convencional podría pasar por alto. Para el régimen ecuatoriano, esta perspectiva permite considerar que un tratamiento puede cumplir determinadas exigencias técnicas y, pese a ello, producir riesgos diferenciados entre grupos. La responsabilidad proactiva demanda identificar también esas consecuencias antes de desplegar sistemas.

El cumplimiento regulatorio basado en riesgos no significa reducir garantías para tratamientos considerados menores, sino asignar controles proporcionales a las amenazas identificadas. La LOPDP mantiene derechos y principios aplicables, mientras permite estructurar medidas según características de cada operación. El Reglamento General contribuye a ordenar análisis, seguridad y mecanismos preventivos. Esta metodología favorece decisiones justificables: una organización debe poder explicar qué riesgos encontró, qué medidas adoptó y por qué considera razonable el nivel residual existente para los titulares.

La documentación cumple una función jurídica decisiva dentro de este modelo. Registrar evaluaciones, medidas de seguridad, decisiones técnicas y revisiones permite demostrar que la protección fue incorporada a la gestión institucional. Friedewald et al. (2021) muestran que las evaluaciones de impacto adquieren utilidad cuando dialogan con prácticas organizacionales y no permanecen como ejercicios formales. Bajo la LOPDP, la responsabilidad proactiva reclama precisamente esa capacidad demostrativa, donde cumplir significa también conservar evidencia suficiente de las decisiones adoptadas preventivamente.

La responsabilidad proactiva consolida una gobernanza donde proteger datos implica anticipar, evaluar, documentar y revisar. La LOPDP y su Reglamento General articulan análisis de riesgos, seguridad, protección desde el diseño y evaluaciones de impacto como piezas relacionadas. Kasirzadeh y Clifford (2021) incorporan la equidad al examen preventivo, mientras Friedewald et al. (2021) destacan su dimensión práctica. Este modelo desplaza el cumplimiento desde una obediencia formal hacia una gestión permanente orientada a preservar derechos verificables.

Tabla 3
Dimensiones jurídicas de la protección de datos personales y la gobernanza de la información en Ecuador

Dimensión jurídica y tecnológica	Alcance regulatorio y garantías aplicables
Protección de datos como derecho autónomo	Reconoce a la persona facultades de acceso, decisión y protección respecto de sus datos. Su autonomía permite tutelar la información personal más allá de la intimidad y exige límites jurídicos frente a tratamientos realizados por actores públicos y privados.
Consentimiento y legitimación del tratamiento	El consentimiento debe responder a una manifestación libre, específica, informada e inequívoca. Junto con otras bases de legitimación previstas legalmente, permite determinar cuándo el tratamiento posee fundamento jurídico y qué obligaciones de transparencia corresponden al responsable.

Perfilamiento e inferencias algorítmicas	La construcción automatizada de perfiles puede atribuir preferencias, comportamientos, capacidades o riesgos a personas identificadas o identificables. La protección jurídica comprende derechos del titular, transparencia, proporcionalidad y garantías frente a determinadas decisiones automatizadas.
Datos biométricos y vigilancia tecnológica	El tratamiento de rasgos biométricos demanda protección reforzada debido a su capacidad identificadora y permanencia. Reconocimiento facial, autenticación biométrica y vigilancia requieren valorar legitimidad, necesidad, proporcionalidad, seguridad y posibles afectaciones a la intimidad y dignidad.
Transferencias internacionales y servicios en la nube	La circulación transfronteriza de datos exige mecanismos que preserven las garantías reconocidas al titular. El empleo de infraestructura distribuida plantea cuestiones sobre jurisdicción, proveedores internacionales, continuidad de la protección, seguridad y soberanía informacional.
Responsabilidad proactiva y gestión de riesgos	Responsables y encargados deben adoptar medidas preventivas, documentadas y verificables. El análisis de riesgos, la protección desde el diseño y las evaluaciones de impacto permiten anticipar afectaciones y adecuar las medidas organizativas y técnicas a las características del tratamiento.

Nota. La tabla organiza los principales ámbitos examinados en el Capítulo 3 a partir de la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la Constitución de la República del Ecuador y la Ley Orgánica para la Transformación Digital y Audiovisual, según corresponda a cada dimensión.

Capítulo 4:

Nuevos derechos digitales y tutela jurídica de la persona conectada

La transformación digital ha desplazado buena parte de la experiencia humana hacia espacios mediados por datos, plataformas, algoritmos y sistemas inteligentes. Allí se conversa, trabaja, recuerda y construye identidad. También allí pueden producirse nuevas formas de afectación jurídica. Pangrazio y Sefton-Green (2021) distinguen los derechos digitales de la ciudadanía y la alfabetización digitales, una precisión útil para comprender que la vida conectada demanda garantías exigibles, además de capacidades personales para desenvolverse responsablemente en entornos tecnológicos contemporáneos.

Desde esa perspectiva, los derechos digitales no constituyen una ruptura completa con el constitucionalismo, sino una ampliación de sus preguntas tradicionales ante relaciones tecnológicamente mediadas. Dignidad, intimidad, identidad, honor, libertad y autonomía mantienen su fuerza normativa, aunque ahora enfrentan tratamientos masivos de datos y representaciones artificiales. Pangrazio y Sefton-Green (2021) permiten advertir que reconocer derechos en ambientes digitales exige distinguir la posición jurídica de la persona respecto de las competencias necesarias para ejercerla de manera efectiva, consciente y libre.

La identidad ofrece una muestra especialmente sensible de esta transformación. Una voz, una fotografía o ciertos gestos pueden convertirse en insumos para sistemas capaces de reproducir rasgos personales con notable fidelidad. Lee y Sun (2026) examinan la clonación vocal desde los derechos de personalidad, publicidad y protección de datos, revelando tensiones jurídicas que desbordan las categorías tradicionales. La pregunta adquiere entonces una dimensión íntima: qué capacidad conserva una persona para decidir quién puede representarla cuando su presencia admite reproducción artificial.

La vida conectada también ha modificado las fronteras temporales del trabajo. Mensajes, correos y plataformas

corporativas mantienen abierta la comunicación cuando la jornada debería haber concluido. En Ecuador, el Acuerdo Ministerial MDT-2022-237 reconoce lineamientos específicos sobre desconexión laboral en el teletrabajo (Ministerio del Trabajo del Ecuador, 2022). Esta regulación recuerda que la disponibilidad técnica no equivale a disponibilidad jurídica permanente. El descanso conserva valor propio y requiere límites frente a prácticas digitales capaces de extender silenciosamente obligaciones laborales cotidianas.

Figura 10

Tutela jurídica de los nuevos derechos digitales



Otra tensión aparece entre memoria personal y permanencia informativa. Internet conserva aquello que antes podía perder visibilidad con el transcurso del tiempo: noticias, fotografías, registros y referencias permanecen indexados durante años. Kiriak (2021) estudia el derecho al olvido como respuesta jurídica frente a esa persistencia, considerando su relación con otros derechos e intereses legítimos. La cuestión exige equilibrio, pues proteger la trayectoria individual no autoriza borrar

indiscriminadamente información relevante para libertad de expresión, transparencia, historia o memoria colectiva.

Más profunda resulta la inquietud planteada por las neurotecnologías. Cuando determinados dispositivos registran señales cerebrales, la protección jurídica alcanza una esfera cercana a la interioridad mental. Moreira (2026) compara perspectivas regulatorias sobre neuroderechos y examina distintas vías de reforma frente al avance neurotecnológico. Para Ecuador, la discusión debe construirse con prudencia desde dignidad, integridad, intimidad, autonomía y protección de datos sensibles, sin atribuir al ordenamiento nacional una legislación general autónoma de neuroderechos actualmente inexistente en el país.

La inteligencia artificial generativa agrega otra capa de complejidad al producir imágenes, voces y videos hiperrealistas capaces de alterar la percepción de autenticidad. Romero-Moreno (2025) relaciona la detección de deepfakes con la salvaguarda de derechos fundamentales, mientras Blurred realities (2026) examina respuestas jurídicas frente a fraude, desinformación y apropiación de representaciones personales. La integridad informacional adquiere entonces relevancia porque la confianza pública depende, en buena medida, de poder distinguir entre acontecimientos registrados y acontecimientos fabricados artificialmente.

Estas transformaciones encuentran en Ecuador un entramado jurídico que permite construir respuestas desde diferentes ámbitos. La Constitución protege identidad, intimidad, honor, imagen, voz, datos personales, integridad y libertad de expresión; la legislación de protección de datos desarrolla facultades de control sobre información personal. A ello se añaden reglas laborales, civiles, penales, de telecomunicaciones y propiedad intelectual. No existe una respuesta normativa única. La tutela de la persona conectada requiere interpretar estas disposiciones de manera coordinada ante cada afectación tecnológica concreta.

Con todo, reconocer nuevos derechos digitales no debería convertirse en una carrera por multiplicar denominaciones jurídicas. Moreira (2026) evidencia que incluso ante los neuroderechos existen diferentes caminos regulatorios, mientras Kiriiak (2021) muestra que el olvido digital demanda ponderación entre posiciones concurrentes. Algo semejante ocurre con identidad, desconexión e integridad informacional. En ocasiones será necesario desarrollar categorías nuevas; en otras, bastará reinterpretar garantías existentes. Lo determinante será preservar protección efectiva frente a poderes tecnológicos capaces de alterar autonomía, reputación o libertad.

Este capítulo aborda, por tanto, a la persona conectada desde una premisa común: la tecnología transforma las condiciones materiales en que los derechos se ejercen, pero no reduce la dignidad que los fundamenta. Pangrazio y Sefton-Green (2021), Lee y Sun (2026), Kiriiak (2021), Moreira (2026) y Romero-Moreno (2025) permiten observar distintas facetas de esa transformación. Identidad digital, desconexión, olvido, neuroderechos e integridad informacional conforman una agenda jurídica donde innovación y libertad necesitan encontrarse bajo garantías democráticas.

4.1. Configuración jurídica de los derechos digitales en el constitucionalismo contemporáneo

La configuración jurídica de los derechos digitales parte de una premisa constitucional: la dignidad humana conserva plena vigencia cuando la vida social se desplaza hacia entornos tecnológicos. En Ecuador, los derechos a la intimidad, protección de datos, honor, comunicación y acceso a información ofrecen bases para responder a relaciones mediadas por plataformas. Pangrazio y Sefton-Green (2021) distinguen los derechos digitales de la ciudadanía y alfabetización digitales, atribuyéndoles una función normativa vinculada con garantías exigibles individual.

La Constitución ecuatoriana reconoce una arquitectura de protección que adquiere renovado significado ante la digitalización. El artículo 66 ampara la intimidad personal y familiar, la protección de datos personales, el honor y la inviolabilidad de las comunicaciones (Constitución de la República del Ecuador, 2008). Estas garantías no nacieron necesariamente para internet, pero su fuerza normativa alcanza bases de datos, redes sociales, servicios automatizados y comunicaciones electrónicas, donde la personalidad queda expuesta a tratamientos tecnológicos intensivos.

Dentro de esa arquitectura, la protección de datos posee autonomía jurídica y una dimensión de autodeterminación informativa. La Ley Orgánica de Protección de Datos Personales establece como objeto garantizar el acceso, la decisión y la protección respecto de información personal (LOPD, 2021, art. 1). Esta formulación desplaza la mirada desde la mera confidencialidad hacia el poder de la persona sobre sus datos. Hay aquí una transformación relevante: la información personal deja de ser materia disponible.

El hábeas data completa este entramado mediante una garantía jurisdiccional vinculada con la persona conectada. El artículo 92 constitucional permite conocer la existencia de datos personales, acceder a ellos e identificar su uso, propósito, origen y destino, además de solicitar actualización, rectificación, eliminación o anulación (Constitución de la República del Ecuador, 2008). En ambientes digitales, esta garantía adquiere valor frente a archivos extensos, perfiles automatizados y tratamientos capaces de prolongarse más allá del conocimiento individual.

La noción de derechos digitales tampoco debe confundirse con las competencias necesarias para desenvolverse en internet. Pangrazio y Sefton-Green (2021) advierten que derechos digitales, ciudadanía digital y alfabetización digital responden a marcos normativos distintos, aunque mantienen relaciones. La diferencia

importa jurídicamente: conocer una plataforma o participar responsablemente en línea no reemplaza las obligaciones estatales y privadas de respetar derechos. La destreza tecnológica puede fortalecer autonomía, pero la garantía jurídica permanece exigible aun ante desigualdades educativas.

La Ley Orgánica para la Transformación Digital y Audiovisual amplía el horizonte institucional al promover servicios digitales y mecanismos de transformación (Ley Orgánica para la Transformación Digital y Audiovisual, 2023). Su lectura constitucional exige que la eficiencia tecnológica permanezca vinculada con igualdad, accesibilidad, seguridad y protección de la persona. Digitalizar procedimientos no equivale a reducir garantías; por el contrario, obliga a diseñar canales capaces de preservar derechos durante cada interacción entre ciudadanía, administración y proveedores tecnológicos.

La conectividad también integra esta construcción jurídica porque el ejercicio de libertades contemporáneas depende de infraestructuras modernas robustas de comunicación realmente seguras. La Ley Orgánica de Telecomunicaciones vincula la prestación de servicios con privacidad y protección de datos, imponiendo deberes de seguridad a los operadores (Ley Orgánica de Telecomunicaciones, 2015). Esta relación revela que el acceso técnico y la tutela jurídica deben avanzar juntos: una conexión desprovista de garantías puede ampliar exposición, vigilancia o vulnerabilidad.

El acceso a información pública adquiere una dimensión digital ligada al control democrático. La Ley Orgánica de Transparencia y Acceso a la Información Pública refuerza obligaciones de publicidad y acceso mediante herramientas compatibles con una administración digital (LOTAIP, 2023). Desde la perspectiva constitucional, la tecnología puede reducir barreras entre instituciones y ciudadanía, pero también crear nuevas exclusiones cuando los sistemas resultan inaccesibles. La tutela

efectiva requiere información disponible, comprensible, íntegra y susceptible de verificación pública.

La configuración contemporánea de estos derechos reclama interpretar normas tradicionales frente a prácticas de datificación más penetrantes. Pangrazio y Sefton-Green (2021) observan que la vida digital enfrenta vigilancia de datos, transacciones predeterminadamente digitales y tensiones sobre la agencia individual. En Ecuador, esta lectura dialoga con los principios de seguridad, transparencia, pertinencia y responsabilidad previstos por la LOPDP (2021). El derecho debe atender no únicamente daños consumados, sino determinadas estructuras tecnológicas capaces de condicionar decisiones personales.

En el constitucionalismo contemporáneo, los derechos digitales pueden entenderse como proyecciones, especificaciones y nuevas formulaciones de la dignidad frente al poder tecnológico. La experiencia ecuatoriana muestra un entramado compuesto por Constitución, protección de datos, transformación digital, telecomunicaciones y transparencia, cuyas piezas deben interpretarse de manera articulada. La distinción propuesta por Pangrazio y Sefton-Green (2021) ayuda a mantener claridad conceptual: los derechos establecen posiciones jurídicas exigibles, mientras ciudadanía y alfabetización aportan capacidades para ejercerlas con autonomía.

4.2. Derecho a la identidad digital y protección frente a la suplantación mediante inteligencia artificial

La identidad digital constituye una proyección jurídica de la personalidad cuando atributos humanos circulan mediante sistemas informáticos, plataformas y modelos de inteligencia artificial. Nombre, rostro, voz, gestos y datos biométricos permiten reconocer a una persona y, al mismo tiempo, reproducirla artificialmente. La Constitución ecuatoriana protege la identidad

personal y colectiva, junto con honor, buen nombre, imagen y voz (Constitución de la República del Ecuador, 2008, art. 66). Esta protección adquiere renovada relevancia ante imitaciones sintéticas.

La inteligencia artificial generativa ha alterado profundamente las posibilidades de apropiación de atributos personales. Una grabación breve puede alimentar sistemas capaces de producir expresiones vocales convincentes sin intervención posterior del titular. Lee y Sun (2026) examinan esta realidad desde los derechos de personalidad, publicidad y protección de datos, mostrando que la voz requiere tutela frente a usos artificiales no consentidos. La cuestión jurídica trasciende la falsificación técnica: compromete reconocimiento, autonomía y control sobre representaciones individuales.

En Ecuador, el derecho constitucional a la identidad ofrece un fundamento relevante frente a la suplantación digital. El artículo 66 reconoce el derecho a la identidad personal y colectiva, que comprende nombre, apellido y características materiales e inmateriales de la identidad (Constitución de la República del Ecuador, 2008). Bajo esta perspectiva, una representación artificial atribuida falsamente a determinada persona puede lesionar elementos mediante los cuales aquella es reconocida socialmente, especialmente cuando reproduce rasgos inequívocamente individualizadores.

La voz merece atención particular porque funciona simultáneamente como expresión personal, elemento identificador y dato susceptible de tratamiento automatizado. Lee y Sun (2026) sostienen que la clonación vocal plantea insuficiencias cuando las categorías jurídicas existentes protegen fragmentariamente intereses vinculados con identidad y personalidad. En el ordenamiento ecuatoriano, la LOPDP reconoce los datos biométricos dentro de categorías especiales cuando permiten

identificar inequívocamente a una persona (Ley Orgánica de Protección de Datos Personales [LOPDP], 2021, art. 25).

El consentimiento ocupa una posición determinante cuando sistemas inteligentes utilizan datos personales para reproducir atributos identificables. La LOPDP exige que aquel sea libre, específico, informado e inequívoco, además de permitir su revocación (LOPDP, 2021). Haber publicado una fotografía, video o grabación no convierte necesariamente esos elementos en materia disponible para cualquier tratamiento. La diferencia resulta decisiva: exposición pública y autorización jurídica no son equivalentes, especialmente cuando la reutilización persigue crear réplicas artificiales con apariencia de autenticidad personal.

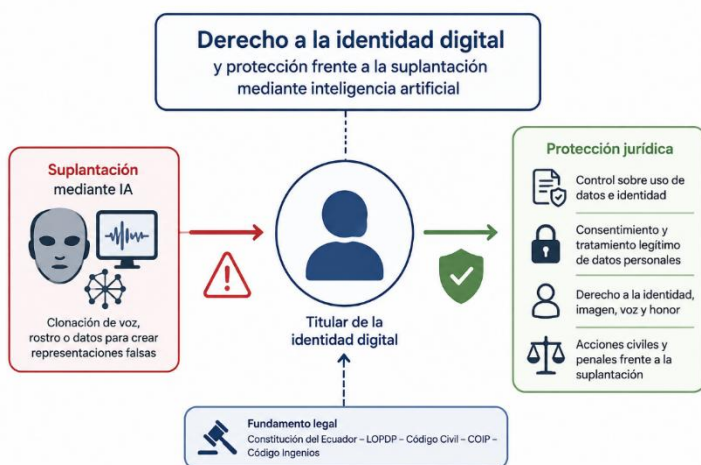
La afectación tampoco termina en el tratamiento indebido de datos. Una réplica artificial puede comprometer honor, reputación, intimidad, imagen y voz, bienes expresamente protegidos por la Constitución (2008, art. 66). Lee y Sun (2026) explican que la clonación mediante inteligencia artificial tensiona categorías jurídicas construidas antes de la reproducción sintética altamente convincente. De allí nace una pregunta incómoda: quién controla una identidad técnicamente reproducible cuando terceros pueden hacerla hablar, actuar o recomendar productos sin autorización.

El Código Civil aporta otra dimensión protectora mediante las reglas generales de responsabilidad derivadas del daño. Cuando una suplantación artificial ocasiona perjuicios patrimoniales o extrapatrimoniales, la respuesta jurídica puede proyectarse hacia reparación, siempre que concurren los presupuestos correspondientes. Esta vía resulta relevante porque una identidad manipulada puede afectar relaciones laborales, familiares o comerciales. La reparación, sin embargo, enfrenta dificultades particulares cuando la difusión digital multiplica copias, intermediarios y audiencias antes de que la persona afectada conozca el hecho.

Cuando la identidad sintética sirve para obtener dinero, credenciales, bienes o ventajas mediante engaño, la valoración jurídica puede trasladarse al ámbito penal. El Código Orgánico Integral Penal tipifica conductas relacionadas con estafa, apropiación fraudulenta por medios electrónicos y falsificación, según los elementos presentes en cada caso (COIP, 2014). La inteligencia artificial opera entonces como instrumento de ejecución. No toda imitación configura delito, pero determinadas prácticas adquieren relevancia penal cuando satisfacen íntegramente los elementos del tipo aplicable.

Figura 11

Protección jurídica de la identidad digital



Existe además una dimensión vinculada con contenidos intelectualmente protegidos. Una operación de suplantación puede reutilizar fotografías, interpretaciones, grabaciones u otras creaciones sujetas al régimen establecido por el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (Código Ingenios, 2016). La protección de identidad y la propiedad intelectual responden a intereses jurídicos distintos,

aunque pueden coincidir ante una misma conducta. Esa concurrencia exige distinguir cuidadosamente personalidad, datos personales y derechos sobre contenidos utilizados.

La tutela de la identidad digital frente a inteligencia artificial requiere, en consecuencia, una lectura articulada del ordenamiento ecuatoriano. Constitución, LOPDP, responsabilidad civil, derecho penal y propiedad intelectual ofrecen respuestas complementarias, aunque cada régimen conserva requisitos propios. Lee y Sun (2026) muestran que la clonación vocal obliga a reconsiderar el control jurídico sobre atributos humanos reproducibles. En Ecuador, proteger identidad digital significa preservar la facultad personal de decidir qué representación puede legítimamente hablar, aparecer o actuar en nombre propio.

4.3. Derecho a la desconexión digital y límites jurídicos a la disponibilidad permanente

El derecho a la desconexión digital expresa una respuesta jurídica frente a la expansión del trabajo más allá de sus fronteras temporales tradicionales. Teléfonos, plataformas corporativas y sistemas de mensajería permiten mantener vínculos laborales después de concluida la jornada, pero esa posibilidad técnica no convierte al trabajador en sujeto permanentemente disponible. En Ecuador, el Acuerdo Ministerial MDT-2022-237 reconoce lineamientos de desconexión laboral aplicables al teletrabajo, vinculando organización tecnológica, jornada y respeto efectivo del tiempo destinado al descanso personal.

La disponibilidad permanente altera una distinción histórica del derecho laboral: tiempo de trabajo y tiempo de descanso. En modalidades digitales, esa frontera puede desdibujarse mediante correos nocturnos, mensajes durante fines de semana o requerimientos aparentemente menores que mantienen activa la atención profesional. El Acuerdo Ministerial MDT-2022-237 procura ordenar esta relación mediante directrices

específicas para el contrato de teletrabajo y la desconexión laboral (Ministerio del Trabajo del Ecuador, 2022). La regla protege una libertad temporal jurídicamente reconocible.

La desconexión no equivale meramente a apagar dispositivos. Su dimensión jurídica reside en impedir que la tecnología transforme el descanso en una prolongación silenciosa de obligaciones profesionales. La regulación ecuatoriana dispone que el empleador establezca una política de desconexión destinada a garantizar el tiempo durante el cual el teletrabajador no estará obligado a responder comunicaciones laborales (Ministerio del Trabajo del Ecuador, 2022). El punto resulta significativo: descansar requiere también quedar temporalmente fuera de las expectativas empresariales de respuesta.

Este derecho introduce límites frente al poder de dirección ejercido mediante tecnologías digitales. La facultad empresarial de organizar actividades conserva legitimidad, aunque encuentra fronteras cuando invade períodos destinados al descanso. El Acuerdo Ministerial MDT-2022-237 establece lineamientos que obligan a considerar la desconexión dentro de la organización del teletrabajo (Ministerio del Trabajo del Ecuador, 2022). En términos laborales, la herramienta tecnológica no amplía por sí misma las potestades patronales ni elimina las restricciones temporales asociadas con la jornada pactada legalmente.

La protección adquiere especial importancia ante prácticas empresariales que confunden flexibilidad con disponibilidad ilimitada. El teletrabajo permite distribuir ciertas actividades mediante tecnologías de información y comunicación, pero conserva obligaciones relacionadas con jornada, descanso y condiciones laborales. Desde la regulación ecuatoriana, la desconexión funciona como contrapeso frente a una flexibilidad que podría volverse invasiva (Ministerio del Trabajo del Ecuador, 2022). Hay una diferencia jurídica evidente entre organizar

autónomamente el tiempo y permanecer pendiente, durante horas, de instrucciones inesperadas.

Los riesgos psicosociales digitales permiten comprender otra dimensión del problema. La recepción reiterada de comunicaciones laborales fuera de jornada puede mantener al trabajador en estado de atención, incluso cuando ninguna tarea material está ejecutándose. Por ello, estudiar la desconexión junto con tales riesgos permite advertir que el descanso posee una dimensión cualitativa. El Acuerdo Ministerial MDT-2022-237 orienta la regulación hacia períodos efectivos de desconexión (Ministerio del Trabajo del Ecuador, 2022), evitando que la conectividad vacíe materialmente el descanso reconocido.

La eficacia de este derecho depende también de la cultura organizacional. Una política escrita pierde capacidad protectora cuando responder mensajes nocturnos determina ascensos, evaluaciones favorables o reconocimiento profesional. En tales circunstancias, la disponibilidad puede parecer voluntaria mientras opera una presión implícita difícil de acreditar. Los lineamientos ecuatorianos sobre desconexión ofrecen una base para ordenar institucionalmente estas prácticas (Ministerio del Trabajo del Ecuador, 2022). El derecho laboral debe observar entonces conductas formales, pero también expectativas empresariales generadas cotidianamente.

Los límites jurídicos a la disponibilidad permanente alcanzan igualmente a mecanismos automatizados de gestión. Plataformas que asignan tareas, generan alertas o registran tiempos pueden extender indirectamente la jornada cuando mantienen requerimientos activos fuera del horario correspondiente. Aunque el Acuerdo Ministerial MDT-2022-237 se ocupa del teletrabajo y la desconexión, sus lineamientos permiten interpretar críticamente estas formas de organización digital (Ministerio del Trabajo del Ecuador, 2022). Automatizar una instrucción no modifica la

naturaleza laboral del requerimiento ni legitima temporalmente su exigencia.

La desconexión requiere mecanismos internos que permitan prevenir incumplimientos y resolver conflictos antes de normalizar prácticas invasivas. Horarios identificables, protocolos de comunicación y reglas frente a situaciones excepcionales pueden contribuir a delimitar las expectativas de disponibilidad. La regulación ecuatoriana coloca la política de desconexión dentro de las responsabilidades vinculadas al teletrabajo (Ministerio del Trabajo del Ecuador, 2022). Esta perspectiva desplaza el problema desde la disciplina individual hacia la organización empresarial: descansar no debería depender de la valentía personal para ignorar mensajes laborales.

En Ecuador, el derecho a la desconexión representa una pieza relevante de la tutela jurídica de la persona conectada. Su fundamento práctico reside en preservar fronteras temporales frente a tecnologías capaces de mantener abierta indefinidamente la relación laboral. El Acuerdo Ministerial MDT-2022-237 aporta lineamientos específicos para esa protección (Ministerio del Trabajo del Ecuador, 2022). La cuestión de fondo permanece profundamente humana: el trabajo digital requiere reglas que reconozcan que disponibilidad tecnológica y disponibilidad jurídica no significan necesariamente lo mismo.

4.4. Derecho al olvido, memoria digital y permanencia de la información en internet

El derecho al olvido plantea una tensión característica de la sociedad digital: la capacidad tecnológica de conservar información durante períodos indefinidos frente al interés personal de evitar que ciertos datos continúen condicionando la vida presente. Kiriak (2021) vincula esta figura con la posibilidad de limitar la persistencia informativa cuando desaparecen razones legítimas para mantener determinados contenidos accesibles. En Ecuador, su análisis

encuentra fundamento constitucional en la protección de datos personales, intimidad, honor y autodeterminación informativa.

Internet modificó profundamente la relación humana con la memoria. Aquello que antes podía perder visibilidad con el paso del tiempo permanece disponible mediante buscadores, archivos, copias y sistemas de indexación. La información adquiere una persistencia capaz de acompañar durante años a la persona involucrada. Kiriak (2021) observa que el derecho al olvido responde precisamente a tensiones derivadas de esa permanencia tecnológica. El problema jurídico consiste en determinar cuándo conservar información deja de resultar legítimo o proporcional.

En el ordenamiento ecuatoriano, la Ley Orgánica de Protección de Datos Personales reconoce el derecho de eliminación cuando concurren determinadas circunstancias relacionadas con el tratamiento (LOPDP, 2021). Esta facultad permite solicitar que datos personales sean suprimidos cuando han dejado de ser necesarios, existe tratamiento ilegítimo o aparecen otros presupuestos previstos legalmente. La eliminación introduce una frontera frente a la memoria digital indiscriminada, aunque su ejercicio permanece sujeto a excepciones destinadas a proteger otros intereses jurídicamente relevantes.

El derecho de oposición complementa esa arquitectura protectora porque permite cuestionar determinados tratamientos atendiendo a circunstancias personales y fundamentos jurídicos aplicables. La LOPDP (2021) reconoce esta facultad dentro del conjunto de derechos atribuidos al titular de información personal. Frente a sistemas digitales que reproducen, clasifican o difunden datos persistentemente, oponerse puede adquirir especial relevancia. No toda permanencia informativa resulta neutral: ciertos tratamientos prolongados pueden alterar reputación, autonomía y oportunidades mucho después del acontecimiento originalmente registrado.

La rectificación cumple una función diferente, aunque estrechamente relacionada con la memoria digital. Una información falsa, incompleta o inexacta puede adquirir apariencia de verdad cuando permanece repetida durante años. La LOPDP (2021) permite al titular solicitar la corrección de datos personales inexactos, fortaleciendo el control sobre su representación informativa. El Reglamento General a la LOPDP desarrolla el marco de ejercicio de los derechos reconocidos legalmente (Reglamento General a la Ley Orgánica de Protección de Datos Personales, 2023).

Figura 12

Tutela del derecho al olvido digital



Sin embargo, hablar de olvido jurídico no significa reconocer una potestad irrestricta para borrar acontecimientos del espacio público. Kiriak (2021) advierte que este derecho requiere ponderación frente a libertad de expresión e intereses informativos legítimos. La Constitución ecuatoriana protege tanto los datos personales y la intimidad como las libertades de expresión, comunicación y acceso a información (Constitución de la República

del Ecuador, 2008). Entre ambas posiciones existe una tensión que debe resolverse atendiendo a proporcionalidad y relevancia pública.

Los archivos de interés público representan un límite particularmente sensible. Documentos históricos, actuaciones estatales, investigaciones periodísticas o registros necesarios para comprender acontecimientos colectivos no pueden evaluarse bajo criterios idénticos a publicaciones privadas carentes de relevancia social. La LOPDP contempla excepciones relacionadas con intereses jurídicamente protegidos, mientras su Reglamento orienta la aplicación de tales disposiciones (LOPDP, 2021; Reglamento General a la LOPDP, 2023). Preservar memoria colectiva puede justificar determinados tratamientos cuando existe fundamento legítimo y proporcional.

También conviene distinguir entre eliminar información de una fuente y reducir su accesibilidad mediante mecanismos de desindexación. Kiriak (2021) examina el derecho al olvido como una categoría jurídica cuya aplicación puede involucrar distintos actores digitales y medidas diferenciadas. Esta distinción resulta relevante porque retirar un resultado asociado a una búsqueda nominativa no equivale necesariamente a destruir el documento originario. La respuesta jurídica puede graduarse, protegiendo al titular sin borrar información cuyo mantenimiento conserve interés público legítimo.

La temporalidad constituye otro criterio significativo para valorar la permanencia informativa. Datos verdaderos y legítimamente publicados pueden perder relevancia con los años, mientras otros conservan interés histórico, jurídico o democrático. Kiriak (2021) destaca que las controversias sobre olvido digital requieren valorar derechos concurrentes, circunstancias particulares y efectos de la difusión. En Ecuador, los principios previstos por la LOPDP permiten examinar necesidad y proporcionalidad del tratamiento, evitando convertir la

disponibilidad tecnológica indefinida en justificación jurídica para conservar cualquier información.

El derecho al olvido revela, en suma, que la memoria digital necesita límites jurídicos compatibles con una sociedad democrática. Constitución, LOPDP y su Reglamento ofrecen instrumentos para eliminar, rectificar u objetar determinados tratamientos, mientras libertad de expresión, acceso a información y conservación de archivos públicos establecen contrapesos indispensables. La perspectiva de Kiriak (2021) permite entender esta figura como ejercicio de ponderación. Proteger a la persona conectada requiere distinguir entre información legítimamente memorable y persistencia digital desproporcionada.

4.5. Neuroderechos, datos neuronales y protección jurídica de la autonomía cognitiva

Los neuroderechos representan una propuesta jurídica dirigida a proteger dimensiones de la persona que las neurotecnologías permiten observar, registrar o eventualmente intervenir. La actividad cerebral puede convertirse en información susceptible de procesamiento, generando interrogantes sobre intimidad, identidad y libertad individual. Moreira (2026) examina distintas perspectivas regulatorias y muestra que todavía existe debate acerca de crear derechos específicos o adaptar garantías existentes. En Ecuador, esta discusión debe partir de la dignidad, integridad, intimidad y autonomía reconocidas constitucionalmente como garantías fundamentales.

Los datos neuronales poseen características que justifican una atención jurídica particularmente cuidadosa. Pueden revelar información relacionada con estados mentales, respuestas fisiológicas, preferencias o condiciones personales, dependiendo de la tecnología empleada y del tratamiento efectuado. Moreira (2026) advierte que el debate regulatorio sobre neuroderechos está relacionado con riesgos derivados del acceso a información

cerebral. Desde Ecuador, la Ley Orgánica de Protección de Datos Personales permite construir protección cuando esos registros identifican o hacen identificable a una persona determinada.

La autonomía cognitiva adquiere relevancia cuando tecnologías externas alcanzan capacidad para inferir, condicionar o intervenir procesos relacionados con decisiones individuales. No se trata únicamente de mantener secretos ciertos pensamientos, sino de preservar un espacio personal frente a interferencias tecnológicas indebidas. La Constitución reconoce el libre desarrollo de la personalidad y protege la integridad personal en diversas dimensiones (Constitución de la República del Ecuador, 2008, art. 66). Estas garantías proporcionan bases interpretativas para tutelar decisiones vinculadas con procesos mentales personales.

La intimidad mental plantea una frontera particularmente delicada. Las tecnologías tradicionales observaban principalmente comportamientos exteriorizados; ciertas neurotecnologías permiten registrar señales producidas antes de convertirse en acciones comunicadas voluntariamente. Moreira (2026) analiza propuestas regulatorias orientadas a responder ante esta capacidad creciente de acceso tecnológico a dimensiones neuronales. En Ecuador, el derecho a la intimidad personal y familiar reconocido constitucionalmente ofrece un fundamento protector (Constitución de la República del Ecuador, 2008, art. 66), aunque su aplicación requerirá interpretación especializada.

La LOPDP adquiere importancia cuando información neuronal constituye dato personal y, especialmente, cuando revela categorías merecedoras de protección reforzada. La legislación ecuatoriana establece un régimen particular para datos sensibles, entre ellos aquellos relativos a salud y datos biométricos destinados a identificar inequívocamente a una persona (LOPDP, 2021). Una señal neuronal no debe calificarse automáticamente bajo una categoría única. Su tratamiento jurídico dependerá de aquello que

permita conocer, de su vinculación individual y de las operaciones realizadas tecnológicamente sobre ella.

El consentimiento representa otra pieza relevante, aunque difícilmente agota la protección requerida. Moreira (2026) muestra que las propuestas sobre neuroderechos buscan responder a escenarios donde las categorías jurídicas tradicionales podrían resultar insuficientes ante determinadas aplicaciones neurotecnológicas. La LOPDP exige condiciones para que el consentimiento resulte válido y reconoce garantías frente al tratamiento de datos personales (LOPDP, 2021). Tratándose de información neuronal, la complejidad técnica obliga a valorar cuidadosamente comprensión, finalidad, proporcionalidad y posibilidades reales de revocación posterior.

La integridad personal también ofrece una vía constitucional para examinar tecnologías capaces de estimular o modificar actividad cerebral. El artículo 66 de la Constitución protege la integridad física, psíquica, moral y sexual de las personas (Constitución de la República del Ecuador, 2008). Esta formulación adquiere especial interés cuando una intervención neurotecnológica puede afectar procesos mentales o conductuales. Moreira (2026) identifica precisamente la integridad mental entre las preocupaciones presentes en propuestas contemporáneas dirigidas a configurar protección jurídica frente a neurotecnologías.

Existe, además, una cuestión distributiva que merece atención. El acceso desigual a tecnologías capaces de potenciar determinadas funciones cognitivas podría producir nuevas diferencias sociales, mientras su utilización obligatoria en ambientes laborales, educativos o comerciales amenazaría libertades individuales. Moreira (2026) compara propuestas de reforma que procuran responder a distintas dimensiones del desarrollo neurotecnológico. Para Ecuador, cualquier regulación futura debería dialogar con igualdad, dignidad y autonomía

constitucionales, evitando que la innovación convierta capacidades mentales humanas en recursos disponibles para terceros.

Conviene mantener prudencia frente a la afirmación de que los neuroderechos constituyen actualmente una categoría legislativa autónoma en Ecuador. El ordenamiento ecuatoriano no cuenta con una ley general específicamente dedicada a ellos. Su tutela debe construirse mediante interpretación de derechos constitucionales y normas de protección de datos aplicables. Moreira (2026) evidencia que internacionalmente existen caminos regulatorios diferentes. Esta diversidad confirma que reconocer riesgos neurotecnológicos no obliga necesariamente a adoptar una única fórmula normativa ni una denominación jurídica uniforme.

La protección jurídica de la autonomía cognitiva obliga, en definitiva, a pensar la persona más allá de sus datos exteriorizados. Cuando la tecnología alcanza señales neuronales, la frontera entre información personal e interioridad humana se vuelve jurídicamente delicada. Constitución y LOPDP ofrecen en Ecuador puntos de partida relevantes, aunque no conforman un régimen autónomo de neuroderechos. La comparación realizada por Moreira (2026) permite advertir alternativas regulatorias. El objetivo permanece claro: preservar dignidad, integridad, intimidad y autodeterminación frente a intervenciones neurotecnológicas.

4.6. Integridad informacional frente a deepfakes, clonación de voz y contenidos sintéticos hiperrealistas

La integridad informacional adquiere relevancia jurídica ante tecnologías capaces de fabricar representaciones audiovisuales difícilmente distinguibles de registros auténticos. Deepfakes, voces clonadas y contenidos sintéticos pueden atribuir declaraciones o conductas inexistentes a personas reales, alterando la relación entre identidad y evidencia. Romero-Moreno (2025) vincula la detección de estas manipulaciones con la protección de derechos

fundamentales. En Ecuador, honor, imagen, identidad e intimidad proporcionan bases constitucionales para responder frente a representaciones artificiales capaces de producir afectaciones personales graves.

Los deepfakes plantean un problema que excede la falsedad del contenido. Su capacidad persuasiva descansa en reproducir atributos reconocibles de una persona, creando una apariencia de presencia que puede engañar incluso a observadores atentos. La literatura reciente vincula estas técnicas con riesgos de fraude, desinformación y apropiación de la persona digital (Blurred realities, 2026). La Constitución ecuatoriana protege honor, buen nombre, imagen y voz, derechos particularmente relevantes cuando una simulación atribuye falsamente actos o expresiones (Constitución, 2008).

La clonación de voz añade una dificultad particular porque transforma un atributo personal reconocible en material susceptible de reproducción automatizada. Grabaciones obtenidas de entrevistas, videos o mensajes pueden alimentar herramientas capaces de generar nuevas expresiones con notable semejanza acústica. Desde la protección de datos, la LOPDP establece salvaguardias reforzadas para categorías sensibles, entre ellas determinados datos biométricos (LOPDP, 2021). La calificación jurídica dependerá del tratamiento efectuado y de la capacidad del registro para identificar inequívocamente al titular.

La protección jurídica tampoco puede reducirse a detectar contenidos manipulados después de su circulación. Romero-Moreno (2025) examina la detección de deepfakes desde una perspectiva orientada a salvaguardar derechos fundamentales, cuestión que desplaza la atención hacia medidas preventivas y mecanismos de autenticidad. La integridad informacional requiere entonces considerar procedencia, trazabilidad y posibilidad de verificar materiales digitales. Esta mirada resulta pertinente cuando imágenes hiperrealistas circulan con velocidad suficiente para

causar daños antes de que una rectificación alcance audiencia comparable.

Existe una tensión inevitable con la libertad de expresión. Los contenidos sintéticos pueden utilizarse legítimamente en creación artística, sátira, educación o producción audiovisual, mientras otros persiguen engañar, difamar o apropiarse de atributos ajenos. La Constitución protege tanto libertad de expresión como honor, intimidad e imagen (Constitución, 2008). Por ello, cualquier respuesta jurídica requiere ponderación. La naturaleza artificial de una pieza no determina por sí misma su ilicitud; importan propósito, identificación, consentimiento, efectos y derechos comprometidos concretamente.

Cuando la fabricación sintética utiliza datos personales, la LOPDP aporta otra capa de protección. Imagen, voz y otros atributos identificables pueden quedar sometidos a operaciones de recopilación, almacenamiento, análisis o generación que constituyan tratamiento de información personal bajo las condiciones legales aplicables (LOPDP, 2021). El consentimiento, la finalidad y la proporcionalidad cobran entonces especial relevancia. Una fotografía disponible públicamente no pierde automáticamente toda protección por encontrarse en internet, ni habilita cualquier reutilización destinada a fabricar identidades digitales convincentes.

La responsabilidad civil adquiere importancia cuando un contenido hiperrealista ocasiona perjuicios verificables. La utilización engañosa de imagen, voz o identidad puede afectar reputación, relaciones profesionales, patrimonio y esfera emocional. Las reglas de responsabilidad previstas en el Código Civil permiten examinar la reparación cuando concurren daño, imputación y los demás presupuestos jurídicos correspondientes (Código Civil, 2005). La dificultad práctica reside frecuentemente en atribuir autoría, medir difusión y contener reproducciones que

continúan circulando aun después de identificarse la manipulación originaria.

La respuesta penal depende de la conducta realizada mediante el contenido sintético y no únicamente de la técnica empleada. Un deepfake puede funcionar como instrumento para engaño patrimonial, extorsión u otras conductas contempladas por el Código Orgánico Integral Penal, siempre que concurren los elementos del tipo correspondiente (COIP, 2014). Blurred realities (2026) relaciona precisamente estas tecnologías con fraude y desinformación. Conviene evitar automatismos: crear una representación sintética y cometer un delito mediante ella constituyen cuestiones jurídicamente diferenciables.

También pueden concurrir derechos intelectuales cuando la producción sintética reutiliza obras, interpretaciones, fotografías, grabaciones u otros contenidos protegidos. El Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación establece el régimen ecuatoriano aplicable a tales bienes (Código Ingenios, 2016). Esta dimensión no reemplaza la tutela de identidad, datos u honor. Una misma pieza puede comprometer intereses jurídicos distintos, razón por la cual resulta necesario identificar separadamente la representación personal afectada y los materiales protegidos empleados.

La integridad informacional frente a contenidos hiperrealistas requiere una respuesta articulada, capaz de preservar confianza sin convertir toda creación sintética en objeto de prohibición. Romero-Moreno (2025) destaca la relación entre detección y protección de derechos, mientras Blurred realities (2026) evidencia implicaciones asociadas con identidad, voz, fraude y desinformación. En Ecuador, Constitución, LOPDP, Código Civil, COIP y Código Ingenios ofrecen vías complementarias. La tarea jurídica consiste en proteger autenticidad personal sin sacrificar expresión legítima e innovación.

Tabla 4*Derechos digitales y mecanismos de tutela jurídica de la persona conectada en Ecuador*

Derecho o ámbito de protección digital	Configuración y tutela jurídica aplicable
Derechos digitales en el constitucionalismo contemporáneo	Proyección de la dignidad, intimidad, protección de datos, comunicación, igualdad y acceso a la información hacia entornos digitales. Su tutela se articula principalmente desde la Constitución, la LOPDP, la Ley Orgánica para la Transformación Digital y Audiovisual y la legislación sobre telecomunicaciones y transparencia.
Identidad digital y protección frente a suplantación mediante IA	Protege nombre, imagen, voz, atributos identificadores y datos personales frente a apropiaciones o representaciones artificiales no autorizadas. La Constitución y la LOPDP constituyen sus principales fundamentos, complementados por responsabilidad civil, COIP y Código Ingenios cuando concurren sus respectivos presupuestos jurídicos.
Desconexión digital y disponibilidad laboral	Delimita la disponibilidad tecnológica del trabajador fuera de la jornada y protege períodos efectivos de descanso frente a comunicaciones y requerimientos laborales digitales. En teletrabajo adquiere especial relevancia el Acuerdo Ministerial MDT-2022-237 del Ministerio del Trabajo, que establece lineamientos relativos al derecho de desconexión laboral.
Derecho al olvido y memoria digital	Comprende mecanismos de eliminación, rectificación y oposición frente al tratamiento de datos cuya permanencia pueda resultar jurídicamente improcedente. Su aplicación requiere ponderación con libertad de expresión, acceso a información y conservación de archivos de interés público, conforme a la Constitución, la LOPDP y su Reglamento General.
Neuroderechos y autonomía cognitiva	Orientados a proteger intimidad mental, integridad, autonomía y datos neuronales frente a determinadas aplicaciones neurotecnológicas. Ecuador carece actualmente de una ley general autónoma de neuroderechos; su tutela debe

	construirse principalmente desde las garantías constitucionales y el régimen de datos personales y sensibles establecido por la LOPDP.
Integridad informacional ante contenidos sintéticos	Busca proteger identidad, honor, imagen, voz, intimidad y autenticidad personal frente a deepfakes, clonación vocal y representaciones hiperrealistas. La respuesta jurídica puede involucrar Constitución, LOPDP, Código Civil, COIP y Código Ingenios, dependiendo de la naturaleza del tratamiento, daño, conducta realizada y contenido utilizado.

Nota. La tabla organiza los principales ámbitos desarrollados en el Capítulo 4 y sus mecanismos de tutela en el Ecuador. La configuración jurídica presentada parte de la Constitución de la República, la Ley Orgánica de Protección de Datos Personales y demás normativa especializada examinada en cada apartado. Elaboración propia.

Capítulo 5:

Regulación tecnológica y construcción del Derecho Digital ecuatoriano

La transformación tecnológica ha dejado de ocupar un espacio periférico dentro del debate jurídico ecuatoriano. La inteligencia artificial, la automatización administrativa y el tratamiento masivo de datos obligan a reconsiderar categorías tradicionales de responsabilidad, control y tutela de derechos. Sourdin (2025) explica que la gobernanza de inteligencia artificial requiere estructuras regulatorias capaces de combinar normas, instituciones y mecanismos de supervisión. Ecuador se encuentra precisamente ante esa tarea: construir respuestas jurídicas propias mientras la innovación avanza con notable rapidez.

El Derecho Digital ecuatoriano se configura mediante normas que nacieron para atender problemas distintos, pero que hoy convergen alrededor de nuevas relaciones tecnológicas. La Constitución, la legislación sobre protección de datos, transformación digital, innovación y servicios financieros tecnológicos proporcionan piezas relevantes, aunque todavía dispersas. Zaidan e Ibrahim (2024) advierten que la gobernanza contemporánea de inteligencia artificial se desarrolla dentro de escenarios regulatorios complejos, donde diversos actores institucionales deben coordinar competencias, responsabilidades y mecanismos efectivos de protección jurídica.

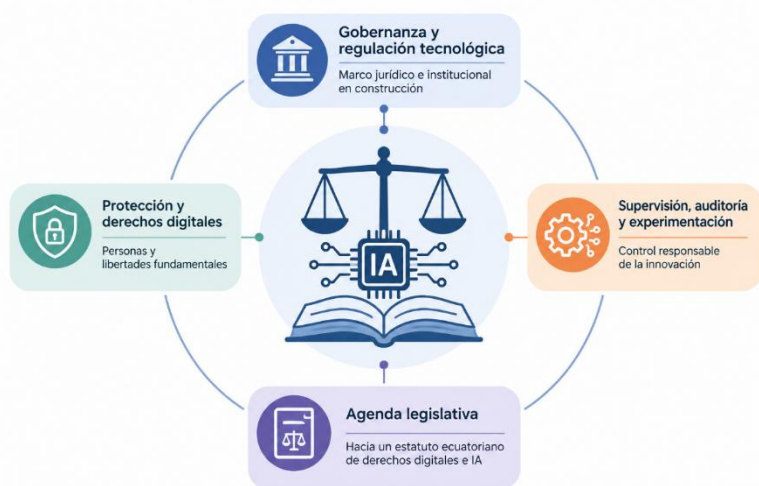
Hablar de regulación tecnológica implica, por ello, abandonar la expectativa de una norma capaz de resolver por sí misma cada tensión producida por sistemas algorítmicos. La cuestión requiere una arquitectura más flexible. Rangone (2025) examina críticamente los modelos regulatorios basados en riesgos y advierte sobre la necesidad de mantener los derechos dentro del análisis regulatorio. Para Ecuador, esta perspectiva permite pensar obligaciones diferenciadas atendiendo al impacto de cada sistema, sin reproducir mecánicamente categorías provenientes de otros ordenamientos.

Esa construcción jurídica demanda mecanismos capaces de convertir principios generales en prácticas verificables. La

transparencia pierde eficacia cuando nadie puede reconstruir decisiones técnicas, identificar responsabilidades o evaluar el cumplimiento normativo. Brogle et al. (2025) relacionan auditoría algorítmica y certificación mediante procedimientos que contrastan sistemas de inteligencia artificial con estándares jurídicos y regulatorios. La trazabilidad adquiere entonces una dimensión probatoria y preventiva: documentar deja de ser una formalidad para convertirse en una garantía frente al poder tecnológico.

Figura 13

Arquitectura del Derecho Digital ecuatoriano



La experimentación regulatoria ocupa también un lugar relevante dentro de este proceso. No toda innovación puede ser comprendida plenamente antes de observar sus efectos en condiciones controladas. Español (2025) plantea los sandboxes regulatorios como espacios de aprendizaje institucional, particularmente valiosos para jurisdicciones que necesitan adaptar modelos tecnológicos y jurídicos a realidades propias. Ecuador cuenta con antecedentes en el ámbito Fintech, experiencia que

permite considerar mecanismos experimentales para inteligencia artificial sin convertir la innovación en territorio exento de derechos.

La regulación, sin embargo, no depende únicamente del contenido de las normas. También importa quién vigila, quién investiga y quién revisa las decisiones adoptadas. Zaidan e Ibrahim (2024) destacan la pluralidad de actores que participan actualmente en la gobernanza de inteligencia artificial. En Ecuador, la protección de datos, la regulación tecnológica, las competencias sectoriales y la Función Judicial forman una trama institucional que requiere canales estables de cooperación, intercambio de información y delimitación precisa de responsabilidades públicas.

Sourdin (2025) añade que una gobernanza adecuada rebasa la aprobación de legislación y comprende auditorías, educación, supervisión y estructuras organizacionales capaces de responder a riesgos cambiantes. Esta mirada resulta especialmente pertinente para un país cuyo modelo regulatorio de inteligencia artificial permanece en construcción. Más que declarar resuelto el problema mediante principios generales, corresponde desarrollar capacidades institucionales que permitan detectar afectaciones, corregir prácticas, revisar decisiones y aprender de la experiencia acumulada durante la aplicación tecnológica cotidiana.

La discusión desemboca necesariamente en los derechos digitales. La expansión de sistemas automatizados modifica las condiciones materiales bajo las cuales las personas ejercen privacidad, igualdad, libertad, autonomía y debido proceso. Ballanca (2025) vincula la inteligencia artificial y el gobierno digital con la necesidad de preservar derechos humanos mediante mecanismos efectivos de responsabilidad algorítmica. Desde esta perspectiva, un futuro estatuto ecuatoriano debería traducir garantías constitucionales hacia escenarios tecnológicos concretos, evitando declaraciones amplias que carezcan de instrumentos reales de exigibilidad.

La agenda legislativa ecuatoriana requiere, además, reconocer aquello que ya existe. La protección de datos personales, la transformación digital, la innovación, la regulación Fintech y diversas disposiciones sectoriales ofrecen fundamentos que no deberían ser desplazados por una futura ley de inteligencia artificial. Español (2025) recuerda la importancia del aprendizaje regulatorio adaptado a las capacidades institucionales de cada jurisdicción. Construir Derecho Digital implica articular estas experiencias, identificar vacíos y desarrollar nuevas obligaciones allí donde las respuestas vigentes resulten insuficientes.

Este capítulo aborda esa construcción desde una perspectiva progresiva: gobernanza jurídica, regulación basada en riesgos, auditoría algorítmica, certificación, experimentación regulatoria, coordinación institucional y agenda legislativa forman partes de una misma conversación. Ballanca (2025) permite comprender que proteger derechos en la era algorítmica requiere relacionar ética, responsabilidad y garantías jurídicas. Ecuador dispone de una oportunidad singular para desarrollar un modelo propio, constitucionalmente orientado, técnicamente informado y abierto a revisión conforme cambien las tecnologías y sus efectos sociales.

5.1. Hacia un modelo ecuatoriano de gobernanza jurídica de la inteligencia artificial

Ecuador necesita una gobernanza jurídica de la inteligencia artificial capaz de crecer con la tecnología sin convertir cada novedad en una carrera legislativa. El punto de partida ya existe: la Constitución coloca la dignidad, la igualdad, la privacidad y la seguridad jurídica en el centro del poder público. Desde esa base, el modelo ecuatoriano puede construirse mediante reglas graduadas, instituciones coordinadas y evaluación permanente, atendiendo la diversidad de riesgos que Sourdin (2025) identifica claramente comparativamente.

La arquitectura nacional no parte de un vacío normativo. La Ley Orgánica para la Transformación Digital y Audiovisual atribuye al ente rector competencias para emitir políticas, directrices y lineamientos en transformación digital, mientras su Reglamento reconoce a la inteligencia artificial entre las tecnologías emergentes vinculadas al desarrollo sostenible (Asamblea Nacional del Ecuador, 2023; Presidencia de la República del Ecuador, 2023). Esta combinación ofrece una base jurídica flexible, aunque todavía dispersa, para ordenar actuaciones institucionales futuras.

Un modelo ecuatoriano razonable debería distinguir entre regulación de la tecnología y gobernanza de sus usos. Sourdin (2025) advierte que gobernar inteligencia artificial rebasa la producción de normas, pues exige estructuras organizacionales, supervisión continua, auditorías, formación y responsabilidades identificables. Esta perspectiva resulta especialmente pertinente para Ecuador, donde la respuesta institucional permanece en construcción. La meta no debería ser copiar esquemas extranjeros, sino traducir aprendizajes comparados a capacidades estatales, sectores productivos, educación y realidades territoriales propias.

La protección de datos personales constituye uno de los pilares ya exigibles. La LOPDP reconoce derechos y obligaciones aplicables al tratamiento automatizado, cuando intervienen datos sensibles, perfiles o decisiones con efectos relevantes (Asamblea Nacional del Ecuador, 2021). En sistemas de inteligencia artificial, estas garantías reclaman trazabilidad, información comprensible, evaluación de riesgos y responsabilidad demostrable. La gobernanza ecuatoriana ganaría coherencia si cada proyecto público incorporara protección de datos desde su diseño durante todo su ciclo operativo.

Importa la dimensión institucional. El Acuerdo MINTEL-MINTEL-2023-0019 dispuso acciones para crear el Comité de Inteligencia Artificial en calidad de mecanismo de consulta, coordinación y articulación entre actores vinculados con esta

materia (MINTEL, 2023). Su valor jurídico no reside en cerrar el debate regulatorio, sino en ofrecer un espacio para organizarlo. Allí puede madurar una gobernanza multisectorial donde Estado, academia, empresas y sociedad civil compartan evidencia, detecten riesgos, formulen estándares y revisen periódicamente las decisiones adoptadas.

La estrategia nacional refuerza esta dirección. Expedida mediante el Acuerdo MINTEL-MINTEL-2025-0030, la EFIA-EC plantea una hoja de ruta orientada al desarrollo, adopción y uso ético y responsable de la inteligencia artificial, con énfasis en capacidades, adopción, gobernanza y ética (MINTEL, 2025). Su existencia marca un avance institucional relevante, pero no equivale a una ley integral de inteligencia artificial. Ecuador dispone hoy de piezas normativas y políticas que todavía requieren articulación, precisión competencial y mecanismos efectivos.

La experiencia comparada invita a evitar dos extremos: una regulación rígida que envejezca pronto y una confianza excesiva en principios voluntarios sin mecanismos de control. Sourdin (2025) distingue aproximaciones de derecho vinculante y marcos de orientación, señalando que ambas pueden convivir dentro de sistemas de gobernanza. Para Ecuador, esa combinación permitiría reservar obligaciones intensas para aplicaciones de mayor riesgo y mantener espacios de experimentación responsable en usos de menor impacto, siempre bajo garantías constitucionales verificables.

En el sector público, la gobernanza debería exigir una justificación reforzada cuando la inteligencia artificial participe en decisiones administrativas o judiciales. La Constitución ecuatoriana obliga a las instituciones a ejercer competencias atribuidas y coordinar acciones para hacer efectivos los derechos (Constitución de la República del Ecuador, 2008). Por ello, ninguna automatización debería diluir la responsabilidad de la autoridad. La

decisión asistida por algoritmos necesita expediente, trazabilidad y supervisión humana y vías efectivas reales de impugnación.

Otro componente es la capacidad de aprender institucionalmente. Sourdin (2025) resalta la educación, el monitoreo y las auditorías entre elementos permanentes de una buena gobernanza de inteligencia artificial. Ecuador podría convertir esos elementos en prácticas mediante evaluaciones de impacto, registros de sistemas de entidades públicas, protocolos de contratación tecnológica y programas de alfabetización para servidores. La regulación dejaría entonces de ser una fotografía estática y funcionaría mediante disciplina de revisión, corrección y rendición de cuentas.

El modelo ecuatoriano, por tanto, conviene entenderlo una construcción jurídica progresiva, apoyada en derechos constitucionales, protección de datos, coordinación institucional y política pública especializada. No existe todavía un régimen legislativo integral y cerrado sobre inteligencia artificial, y esa constatación permite diseñar con prudencia. La tarea pendiente consiste en conectar las normas existentes, definir responsabilidades proporcionales al riesgo y fortalecer supervisión, participación y transparencia, preservando innovación útil sin reducir la ciudadanía a mera fuente de datos.

5.2. Regulación basada en niveles de riesgo y obligaciones diferenciadas para sistemas algorítmicos

La regulación de sistemas algorítmicos basada en niveles de riesgo ofrece a Ecuador una vía para distribuir obligaciones según la intensidad del posible daño. No todas las aplicaciones afectan de igual manera derechos, servicios públicos o decisiones privadas. Rangone (2025) advierte que clasificar riesgos carece de suficiente legitimidad cuando la arquitectura regulatoria pierde de vista los derechos comprometidos. Una futura legislación ecuatoriana

debería vincular cada categoría con garantías exigibles, controles verificables y responsabilidades claramente determinadas.

El referente europeo resulta útil, aunque su trasplante automático sería poco prudente. Rangone (2025) examina críticamente una regulación centrada en categorías de riesgo y muestra tensiones cuando determinadas funciones jurídicas reciben un tratamiento que no refleja plenamente su incidencia institucional. Ecuador requiere criterios propios, contruidos desde su Constitución, estructura administrativa y capacidades de supervisión. La clasificación debería responder a consecuencias previsibles sobre personas y colectivos, antes que reproducir etiquetas diseñadas para otro ordenamiento jurídico democrático.

En Ecuador todavía no existe una ley general de inteligencia artificial que establezca categorías equivalentes a las previstas por el modelo europeo. Esta ausencia, lejos de impedir avances, permite articular criterios desde normas vigentes. La Ley Orgánica de Protección de Datos Personales ofrece parámetros vinculados con tratamientos automatizados, perfiles y decisiones que producen efectos jurídicos (Asamblea Nacional del Ecuador, 2021). Tales disposiciones pueden orientar la futura identificación de aplicaciones algorítmicas merecedoras de mayores salvaguardias.

Una futura clasificación ecuatoriana podría diferenciar aplicaciones de riesgo inadmisibles, alto, moderado y bajo, siempre que esas categorías respondan a evidencia y derechos constitucionales. El nivel más severo debería reservarse para prácticas incompatibles con la dignidad, igualdad o autonomía personal. Los sistemas de alto riesgo requerirían evaluación previa, documentación, trazabilidad y supervisión humana. Rangone (2025) recuerda que el análisis regulatorio pierde fuerza cuando el riesgo se separa de las garantías jurídicas afectadas de manera directa.

Las obligaciones diferenciadas también deberían atender al papel que cumple cada actor dentro del ciclo de vida algorítmico. Quien desarrolla, provee, contrata, implementa o utiliza un sistema posee capacidades distintas para prevenir daños. La Ley Orgánica para la Transformación Digital y Audiovisual aporta una base institucional para políticas públicas de transformación tecnológica (Asamblea Nacional del Ecuador, 2023). Sobre ella podrían establecerse deberes graduados de documentación, evaluación, seguridad, información y vigilancia según funciones y riesgos concretos.

La administración pública merece exigencias reforzadas cuando emplea algoritmos para asignar beneficios, fiscalizar, seleccionar personas o apoyar decisiones con efectos jurídicos. En estos espacios, la eficiencia tecnológica no puede desplazar motivación, transparencia ni posibilidad de contradicción. Rangone (2025) observa que el uso de inteligencia artificial en actividades jurídicas plantea riesgos particulares para derechos y legitimidad institucional. Una regulación ecuatoriana debería exigir registros, evaluaciones de impacto y mecanismos de revisión humana antes de decisiones especialmente sensibles.

La LOPDP aporta una referencia normativa inmediata para graduar obligaciones cuando los sistemas procesan datos personales. Sus principios de propósito, pertinencia, minimización, transparencia y responsabilidad orientan límites jurídicos aplicables al tratamiento algorítmico (Asamblea Nacional del Ecuador, 2021). Cuando intervengan datos sensibles, perfiles extensivos o decisiones automatizadas relevantes, el nivel regulatorio debería elevarse. Esta conexión permitiría que la futura clasificación de riesgos dialogue con garantías existentes, evitando crear un régimen tecnológico aislado del Derecho ecuatoriano vigente.

Las normas sectoriales deberán desempeñar una función complementaria, porque el riesgo algorítmico cambia según el

ámbito de aplicación. Un sistema utilizado para entretenimiento no plantea las mismas consecuencias que otro destinado a salud, educación, crédito, empleo o justicia. Rangone (2025) permite advertir que las categorías generales necesitan lectura institucional para proteger derechos efectivamente. Ecuador podría combinar reglas transversales con obligaciones sectoriales específicas, dejando que autoridades competentes desarrollen estándares técnicos dentro de competencias previamente delimitadas jurídicamente.

Figura 14
Regulación algorítmica según niveles de riesgo



La estrategia ecuatoriana de inteligencia artificial puede servir como espacio de transición entre principios de política pública y futuras obligaciones vinculantes. Su utilidad reside en ordenar prioridades, promover capacidades y preparar mecanismos de gobernanza antes de legislación integral. Sin embargo, una clasificación jurídica de riesgos requiere autoridad normativa, procedimientos definidos y consecuencias ante incumplimientos. La experiencia examinada por Rangone (2025) aconseja mantener

una mirada crítica sobre cualquier taxonomía que privilegie gestión técnica frente a derechos.

El diseño ecuatoriano debería concebir los niveles de riesgo como categorías revisables y no como compartimentos permanentes. Los sistemas cambian, aprenden, reciben nuevos datos y pueden utilizarse para propósitos distintos de aquellos previstos inicialmente. Por ello, las obligaciones tendrían que acompañar todo el ciclo de vida mediante monitoreo, reevaluación y rendición de cuentas. Una regulación proporcional permitiría proteger derechos sin imponer cargas idénticas a aplicaciones heterogéneas, construyendo una respuesta nacional prudente, adaptable y jurídicamente coherente.

5.3. Auditoría algorítmica, trazabilidad y certificación jurídica de sistemas de inteligencia artificial

La auditoría algorítmica puede convertirse en una pieza central del futuro Derecho Digital ecuatoriano, porque permite trasladar principios jurídicos generales hacia verificaciones concretas sobre sistemas de inteligencia artificial. Brogle et al. (2025) vinculan la auditoría con procesos de certificación capaces de contrastar sistemas frente a requisitos regulatorios y estándares aplicables. Para Ecuador, esta perspectiva permitiría examinar riesgos, documentación, funcionamiento y medidas preventivas antes de confiar decisiones relevantes a tecnologías cuya complejidad dificulta el escrutinio ordinario.

Auditar un sistema no equivale a revisar su código de manera aislada. La evaluación requiere observar datos, propósito, diseño, resultados, seguridad y condiciones reales de utilización. Brogle et al. (2025) plantean una certificación dependiente del ámbito específico donde opera la inteligencia artificial, cuestión especialmente visible en sectores sensibles. Esta aproximación resulta pertinente para Ecuador, pues una herramienta clínica, financiera o administrativa demanda criterios de revisión distintos,

aunque todas deban respetar garantías jurídicas comunes previamente establecidas.

La trazabilidad ofrece el hilo documental que permite reconstruir decisiones técnicas y humanas durante el ciclo de vida de un sistema. Sin registros suficientes, determinar responsabilidades puede volverse una tarea incierta. La Ley Orgánica de Protección de Datos Personales exige responsabilidad proactiva y demostrada al responsable del tratamiento, quien debe acreditar medidas apropiadas para cumplir sus obligaciones (Asamblea Nacional del Ecuador, 2021). Esta lógica proporciona fundamento para exigir evidencia verificable cuando algoritmos procesen datos personales.

El Reglamento General de la LOPDP profundiza esa orientación mediante disposiciones relativas a gestión de riesgos, medidas de seguridad y evaluación de impacto en protección de datos (Presidencia de la República del Ecuador, 2023). Trasladadas al campo algorítmico, estas herramientas permiten pensar auditorías documentadas que examinen vulnerabilidades, calidad de datos y consecuencias previsibles. La evaluación jurídica debería comenzar antes del despliegue tecnológico y continuar durante su operación, especialmente cuando cambien datos, funcionalidades o destinatarios.

La certificación jurídica requiere cautela. Un certificado no debería convertirse en una declaración permanente de inocuidad tecnológica, pues los sistemas pueden variar después de su evaluación. Brogle et al. (2025) muestran que la certificación adquiere mayor sentido cuando considera el ámbito concreto de utilización y combina criterios regulatorios con procedimientos verificables. En Ecuador, una futura arquitectura podría establecer certificados temporales, revisiones periódicas y obligaciones de informar modificaciones sustanciales que alteren el perfil jurídico previamente evaluado.

También importa definir quién audita. La independencia del evaluador, su competencia técnica y su conocimiento jurídico condicionan la credibilidad del proceso. Una futura legislación ecuatoriana podría diferenciar auditorías internas, evaluaciones independientes y certificaciones efectuadas por organismos acreditados, según el nivel de riesgo. La Ley Orgánica para la Transformación Digital y Audiovisual proporciona un marco institucional para promover transformación tecnológica (Asamblea Nacional del Ecuador, 2023), aunque todavía requiere desarrollo específico respecto de controles algorítmicos obligatorios.

La trazabilidad debe acompañar tanto decisiones automatizadas como intervenciones humanas relevantes. Registrar versiones del modelo, procedencia de datos, parámetros, incidentes, responsables y cambios permitiría reconstruir el funcionamiento del sistema cuando aparezcan controversias. Brogle et al. (2025) relacionan la evaluación de conformidad con evidencias que permitan contrastar requisitos previamente definidos. Para el Derecho ecuatoriano, esa documentación podría facilitar supervisión administrativa, ejercicio de derechos, investigaciones y determinación de responsabilidades frente a afectaciones concretas posteriores.

Los sectores regulados demandan especial atención porque ya poseen normas técnicas, deberes profesionales y autoridades con competencias propias. Salud, finanzas, telecomunicaciones o servicios públicos no deberían recibir una certificación algorítmica idéntica. La propuesta de Brogle et al. (2025), desarrollada mediante una experiencia piloto sanitaria, evidencia el valor de adaptar requisitos al dominio de aplicación. Ecuador podría articular estándares transversales de inteligencia artificial con controles sectoriales capaces de responder a riesgos particulares y obligaciones jurídicas preexistentes.

Persisten vacíos importantes. La legislación ecuatoriana vigente no configura todavía un régimen general que determine qué

sistemas deben someterse obligatoriamente a auditorías algorítmicas, qué registros deben conservarse o qué procedimiento certifica su conformidad jurídica. La LOPDP y su Reglamento ofrecen instrumentos aprovechables, pero su objeto principal permanece vinculado al tratamiento de datos personales. Una futura ley de inteligencia artificial debería ordenar estas materias mediante criterios proporcionales, autoridades competentes y procedimientos sujetos a revisión periódica.

La auditoría, la trazabilidad y la certificación pueden formar una cadena de confianza jurídica si cada instrumento conserva una función definida. Auditar permite examinar; documentar permite reconstruir; certificar permite acreditar conformidad bajo condiciones determinadas. Ninguna herramienta elimina por sí misma el riesgo. Brogle et al. (2025) permiten comprender la certificación como proceso vinculado al uso específico del sistema. Ecuador tiene la oportunidad de convertir esa lógica en garantías verificables, transparentes y adaptadas a su institucionalidad.

5.4. Sandbox regulatorio como instrumento de experimentación jurídica para tecnologías de alto impacto

El sandbox regulatorio ofrece a Ecuador una vía para experimentar jurídicamente con tecnologías de alto impacto dentro de espacios delimitados, supervisados y temporalmente controlados. Su interés rebasa la promoción empresarial. Español (2025) plantea que estos mecanismos pueden funcionar como entornos de aprendizaje regulatorio, especialmente en jurisdicciones que reciben tecnologías desarrolladas bajo marcos institucionales diferentes. Para el Derecho ecuatoriano, experimentar permitiría producir evidencia antes de establecer obligaciones generales que podrían resultar prematuras, insuficientes o difíciles de aplicar.

La experiencia ecuatoriana posee un antecedente relevante en materia financiera. La Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos incorporó mecanismos orientados a facilitar innovación bajo supervisión regulatoria, abriendo espacio para pruebas controladas dentro del ecosistema Fintech (Asamblea Nacional del Ecuador, 2022). Este precedente demuestra que la experimentación normativa no resulta ajena al ordenamiento nacional. Puede aportar, con las debidas adaptaciones, una referencia institucional para futuros entornos experimentales destinados a inteligencia artificial.

Trasladar ese precedente hacia sistemas algorítmicos exige reconocer diferencias importantes. Una innovación financiera puede comprometer patrimonio, estabilidad o protección del consumidor; una aplicación de inteligencia artificial puede afectar además privacidad, igualdad, autonomía o acceso a servicios públicos. Español (2025) destaca el valor del sandbox cuando genera conocimiento regulatorio mediante interacción entre autoridades y participantes. Ecuador necesitaría, por ello, procedimientos que permitan aprender de cada prueba sin convertir la experimentación tecnológica en reducción injustificada de garantías jurídicas.

El ingreso a un sandbox debería responder a criterios previamente establecidos. No cualquier proyecto requiere tratamiento experimental ni toda innovación merece flexibilización regulatoria. La autoridad tendría que valorar novedad tecnológica, incertidumbre jurídica, impacto esperado, población afectada y medidas de protección disponibles. El aprendizaje regulatorio descrito por Español (2025) adquiere sentido cuando existe una pregunta institucional concreta que la prueba pretende resolver. Experimentar por experimentar aportaría poco al Derecho y podría trasladar riesgos innecesarios hacia ciudadanos participantes.

La autorización temporal tampoco debería entenderse como suspensión general de las normas vigentes. Los derechos constitucionales, las obligaciones de protección de datos y las reglas sectoriales continuarían delimitando la experimentación. El precedente Fintech ecuatoriano permite apreciar que la innovación regulada requiere intervención de autoridades competentes y condiciones específicas (Asamblea Nacional del Ecuador, 2022). Para inteligencia artificial, cualquier excepción autorizada tendría que estar jurídicamente delimitada, motivada, supervisada y acompañada por mecanismos inmediatos de corrección frente a eventuales afectaciones.

Figura 15
Sandbox regulatorio



Un sandbox de inteligencia artificial debería producir documentación aprovechable para futuras decisiones regulatorias. Informes de desempeño, incidentes, riesgos detectados, medidas correctivas y resultados de supervisión permitirían transformar una experiencia particular en conocimiento institucional. Español (2025) concibe estos entornos desde una perspectiva centrada en

aprendizaje, especialmente valiosa para países con capacidades regulatorias en desarrollo. Ecuador podría emplear esa información para formular estándares propios, evitando depender enteramente de modelos extranjeros contruidos bajo condiciones económicas e institucionales diferentes.

La selección de participantes merece igual atención. Empresas grandes, emprendimientos, universidades e instituciones públicas poseen capacidades desiguales para acceder a procesos experimentales. Un diseño concentrado en actores con mayores recursos podría convertir el sandbox en ventaja competitiva antes que en herramienta de aprendizaje público. Español (2025) invita a considerar las particularidades de jurisdicciones no centrales. Bajo esa mirada, Ecuador debería garantizar criterios transparentes de acceso, acompañamiento técnico y difusión de aprendizajes que benefician al ecosistema regulatorio nacional.

Las tecnologías de alto impacto requieren además mecanismos claros de salida. Al concluir la prueba, la autoridad debería decidir si autoriza continuidad, exige modificaciones, dispone nuevas evaluaciones o impide el despliegue. El sandbox adquiere valor jurídico cuando sus resultados producen consecuencias institucionales comprensibles. La experiencia Fintech ofrece un punto de referencia para estructurar relaciones entre innovación y supervisión sectorial. En inteligencia artificial, esas decisiones deberían quedar motivadas, documentadas y disponibles para revisión cuando afecten derechos o intereses legítimos.

La coordinación entre autoridades será especialmente relevante cuando una aplicación experimental atraviese varios sectores. Un sistema algorítmico puede procesar datos personales, prestar servicios financieros y utilizar infraestructura digital al mismo tiempo. Ninguna autoridad debería observar únicamente una fracción del riesgo. Español (2025) destaca el aprendizaje institucional como componente del sandbox. Ecuador podría

aprovechar esta herramienta para desarrollar cooperación entre reguladores, compartir conocimiento técnico y detectar vacíos competenciales antes de que determinadas tecnologías alcancen despliegues masivos en el país.

El sandbox regulatorio puede convertirse, entonces, en un laboratorio jurídico donde Ecuador ensaye respuestas antes de transformarlas en reglas generales. El precedente Fintech demuestra que existe experiencia normativa interna para construir este instrumento, mientras Español (2025) aporta una lectura orientada al aprendizaje regulatorio en jurisdicciones con necesidades propias. Su legitimidad dependerá de límites claros, supervisión efectiva, transparencia y protección de derechos. Bien diseñado, permitiría que la innovación también enseñe al Estado a regular responsablemente.

5.5. Coordinación entre autoridades de protección de datos, órganos judiciales y entidades de regulación tecnológica

La gobernanza ecuatoriana de inteligencia artificial requiere instituciones capaces de actuar coordinadamente cuando una misma tecnología compromete datos personales, derechos fundamentales y competencias sectoriales. Zaidan e Ibrahim (2024) describen un panorama regulatorio caracterizado por múltiples actores y marcos que interactúan frente al desarrollo acelerado de estos sistemas. Para Ecuador, la respuesta jurídica no pasa necesariamente por multiplicar organismos, sino por delimitar atribuciones, establecer canales permanentes de cooperación y prevenir decisiones administrativas contradictorias entre autoridades públicas competentes.

La Superintendencia de Protección de Datos Personales ocupa una posición relevante cuando los sistemas algorítmicos procesan información personal. La LOPDP le atribuye funciones de vigilancia, control y potestad sancionadora dentro de su ámbito

material (Asamblea Nacional del Ecuador, 2021). Sin embargo, una aplicación de inteligencia artificial puede involucrar simultáneamente telecomunicaciones, finanzas, salud o administración pública. La coordinación permitiría conservar especialidades institucionales mientras se construyen respuestas comunes ante tratamientos tecnológicos que atraviesan fronteras regulatorias tradicionales con frecuencia.

La Función Judicial representa otro componente indispensable de esta arquitectura. La Constitución garantiza tutela judicial efectiva, debido proceso y seguridad jurídica, principios que adquieren especial importancia cuando decisiones automatizadas afectan derechos (Constitución de la República del Ecuador, 2008). Los jueces no reemplazan a reguladores técnicos, pero deben conservar capacidad efectiva para revisar actuaciones administrativas, valorar evidencia algorítmica y ordenar reparaciones. La especialización tecnológica puede fortalecer esta función sin debilitar independencia, imparcialidad ni competencias constitucionalmente reconocidas.

La cooperación institucional requiere reglas claras sobre intercambio de información. Un regulador puede conocer incidentes técnicos mientras otro dispone de antecedentes vinculados con protección de datos o afectaciones sectoriales. Zaidan e Ibrahim (2024) destacan que la gobernanza contemporánea de inteligencia artificial demanda respuestas capaces de relacionar actores y estructuras regulatorias diversas. Ecuador podría establecer protocolos que permitan compartir información pertinente, preservando confidencialidad, secreto profesional, protección de datos y garantías procesales de las personas investigadas.

La Ley Orgánica para la Transformación Digital y Audiovisual proporciona elementos para articular políticas estatales vinculadas con transformación tecnológica y gobernanza digital (Asamblea Nacional del Ecuador, 2023). Su aplicación puede

favorecer coordinación entre entidades responsables de modernización pública y organismos con potestades regulatorias específicas. Sin embargo, coordinar no significa concentrar competencias. Una arquitectura institucional equilibrada debería respetar atribuciones legales existentes, definir responsabilidades frente a sistemas algorítmicos y establecer procedimientos para resolver posibles conflictos entre autoridades administrativas.

El Comité de Inteligencia Artificial constituye una experiencia institucional que puede contribuir al diálogo entre actores vinculados con esta tecnología. Su regulación permite concebir espacios de consulta y articulación dentro de la política digital ecuatoriana (MINTEL, 2023). Con todo, un órgano coordinador no sustituye las competencias de supervisión, sanción o revisión judicial establecidas legalmente. Su aporte puede residir en compartir criterios, identificar vacíos regulatorios y facilitar acuerdos técnicos que luego sean aplicados por autoridades competentes.

Sourdin (2025) muestra que la gobernanza de inteligencia artificial comprende estructuras institucionales, supervisión, educación, auditoría y mecanismos de responsabilidad, más allá de reglas sustantivas aisladas. Esta perspectiva resulta valiosa para Ecuador, donde varias autoridades pueden intervenir sobre diferentes dimensiones de un sistema algorítmico. La coordinación debería construirse mediante mesas técnicas, protocolos interinstitucionales, consultas recíprocas y criterios interpretativos compatibles, procurando que ninguna entidad renuncie a las potestades que el ordenamiento le asigna expresamente.

También conviene establecer mecanismos para determinar qué autoridad lidera actuaciones cuando concurren distintas competencias. La protección de datos podría constituir el eje de una investigación, mientras cuestiones financieras, sanitarias o tecnológicas exigirían intervención especializada adicional. Zaidan e Ibrahim (2024) evidencian que la complejidad regulatoria de la

inteligencia artificial reclama enfoques coordinados. En Ecuador, reglas sobre autoridad principal, cooperación técnica y remisión de antecedentes reducirían duplicidades, vacíos de supervisión y cargas administrativas innecesarias para ciudadanos.

La revisión judicial debe cerrar el sistema de coordinación sin convertirse en una instancia meramente formal. Cuando una autoridad adopte decisiones relacionadas con inteligencia artificial, la persona afectada necesita conocer fundamentos suficientes para controvertirlas. La Constitución reconoce el derecho al debido proceso y exige motivación en las decisiones de los poderes públicos (Constitución de la República del Ecuador, 2008). La trazabilidad institucional y algorítmica facilitaría que los jueces examinen legalidad, proporcionalidad y respeto efectivo de derechos fundamentales.

Una gobernanza coordinada requiere, en suma, competencias comprensibles, información compartida bajo garantías y vías judiciales capaces de ofrecer control efectivo. Crear nuevas instituciones sin ordenar relaciones podría aumentar fragmentación antes que resolverla. Sourdin (2025) y Zaidan e Ibrahim (2024) permiten advertir que la gobernanza tecnológica necesita estructuras adaptables y cooperación sostenida. Ecuador puede avanzar mediante una arquitectura donde protección de datos, regulación sectorial, política tecnológica y justicia dialoguen sin perder autonomía ni responsabilidad jurídica propia.

5.6. Agenda legislativa para un estatuto ecuatoriano de derechos digitales e inteligencia artificial

Un estatuto ecuatoriano de derechos digitales e inteligencia artificial debería partir de una premisa sencilla: la tecnología modifica espacios donde los derechos ya existen, pero también plantea formas de afectación que reclaman respuestas jurídicas específicas. Ballanca (2025) vincula gobierno digital, responsabilidad algorítmica y protección de derechos humanos

dentro de una arquitectura regulatoria integrada. Ecuador necesita ordenar normas dispersas, reconocer garantías digitales y establecer responsabilidades aplicables al diseño, implementación y utilización de sistemas inteligentes públicos y privados.

La Constitución ofrece el fundamento normativo para esta agenda legislativa mediante sus garantías de dignidad, igualdad, privacidad, intimidad, libertad de expresión, debido proceso y seguridad jurídica (Constitución de la República del Ecuador, 2008). Un estatuto digital no debería reemplazar estas garantías, sino precisar su aplicación frente a tecnologías capaces de perfilar personas, automatizar decisiones o condicionar oportunidades. La tarea legislativa consiste en traducir principios constitucionales hacia derechos exigibles ante relaciones tecnológicas cada vez más complejas.

La LOPDP y su Reglamento aportan una segunda columna normativa mediante principios de transparencia, responsabilidad proactiva, seguridad y protección frente a determinados tratamientos automatizados (Asamblea Nacional del Ecuador, 2021). Un futuro estatuto debería dialogar con este régimen evitando duplicidades institucionales o contradicciones interpretativas. Ballanca (2025) sostiene que proteger derechos en entornos algorítmicos requiere conectar principios éticos con mecanismos jurídicos de responsabilidad. Esa conexión permitiría ampliar garantías sin debilitar aquellas que ya resultan exigibles actualmente.

La agenda legislativa debería reconocer derechos vinculados con transparencia algorítmica, información comprensible, intervención humana y mecanismos efectivos de impugnación cuando una decisión tecnológica produzca consecuencias relevantes. También merece consideración el derecho a identificar interacciones con sistemas automatizados. Ballanca (2025) relaciona la responsabilidad algorítmica con la necesidad de preservar derechos humanos frente al gobierno

digital. Tales garantías tendrían que formularse con precisión suficiente para evitar declaraciones simbólicas carentes de procedimientos, autoridades responsables o vías concretas de reparación jurídica.

La Ley Orgánica para la Transformación Digital y Audiovisual y su Reglamento ofrecen una base para ordenar políticas de transformación tecnológica del Estado (Asamblea Nacional del Ecuador, 2023). Un estatuto podría complementar ese marco mediante reglas aplicables a contratación, utilización y supervisión de inteligencia artificial en instituciones públicas. El Código Orgánico Administrativo debería conservar un papel relevante cuando algoritmos intervengan en actuaciones administrativas, pues automatizar procedimientos no puede reducir motivación, responsabilidad pública, contradicción ni control jurisdiccional efectivo.

La propuesta también requiere armonización con normas sectoriales. El Código Ingenios aporta elementos vinculados con conocimiento, innovación y propiedad intelectual, mientras la Ley Fintech ofrece antecedentes regulatorios sobre experimentación tecnológica. Las normas laborales relativas a desconexión plantean otra dimensión de los derechos digitales. Ballanca (2025) advierte que la transformación tecnológica atraviesa ámbitos diversos de la vida social. Un estatuto ecuatoriano debería funcionar como marco transversal, dejando regulaciones especializadas para riesgos propios de cada sector económico.

Las materias electoral, penal, civil y de telecomunicaciones requieren tratamiento especialmente cuidadoso. Contenidos sintéticos, suplantaciones digitales, sistemas predictivos, responsabilidad por daños y moderación automatizada plantean preguntas jurídicas diferentes. Pretender resolverlas mediante una cláusula general de inteligencia artificial produciría incertidumbre. La agenda legislativa debería identificar conexiones entre el estatuto y cada cuerpo normativo, estableciendo reformas

puntuales cuando resulten necesarias. Ballanca (2025) enfatiza que la protección digital exige responsabilidad jurídica compatible con derechos humanos fundamentales.

Un estatuto ecuatoriano también debería ordenar obligaciones según riesgos y capacidades de los actores involucrados. Desarrolladores, proveedores, entidades públicas, empleadores y usuarios profesionales ocupan posiciones diferentes frente al funcionamiento algorítmico. Las cargas regulatorias deberían reflejar esas diferencias mediante documentación, evaluaciones de impacto, auditorías, trazabilidad y deberes de información. La responsabilidad no puede desaparecer detrás de la complejidad técnica. Ballanca (2025) sitúa precisamente la rendición de cuentas entre las respuestas necesarias frente al poder creciente de sistemas algorítmicos.

La agenda legislativa necesita además una arquitectura institucional comprensible. Protección de datos, telecomunicaciones, regulación financiera, administración pública y justicia poseen competencias que pueden concurrir sobre una misma tecnología. Antes que crear organismos de manera automática, conviene establecer mecanismos de cooperación, intercambio de información y determinación de autoridad competente. La legislación debería prever procedimientos de supervisión y revisión judicial, preservando independencia institucional. Un derecho digital efectivo depende tanto de garantías sustantivas como de instituciones capaces de hacerlas exigibles.

El futuro estatuto podría convertirse en punto de encuentro entre la tradición constitucional ecuatoriana y una transformación tecnológica que exige respuestas prudentes, revisables y democráticamente legitimadas. Ballanca (2025) recuerda que ética, algoritmos y derechos mantienen una relación que reclama responsabilidad y protección efectiva. Ecuador cuenta con bases normativas dispersas sobre datos, transformación digital,

innovación, trabajo y servicios tecnológicos. La agenda pendiente consiste en integrarlas mediante derechos exigibles, obligaciones proporcionales y mecanismos institucionales capaces de evolucionar responsablemente.

Conclusiones

La transformación digital ha modificado de manera profunda las relaciones entre Derecho, poder y tecnología en el Ecuador, haciendo necesario reconsiderar categorías jurídicas concebidas bajo estructuras predominantemente analógicas. El análisis desarrollado permite concluir que el orden constitucional ecuatoriano dispone de principios capaces de orientar la tutela de la persona frente al poder algorítmico. Dignidad, autonomía, igualdad, intimidad y protección de datos conforman una base relevante. Sin embargo, su eficacia requiere mecanismos jurídicos adaptados a decisiones y relaciones tecnológicamente mediadas.

Las categorías constitucionales vigentes ofrecen fundamentos importantes para responder a los efectos de los sistemas algorítmicos, aunque su formulación general no resuelve todas las particularidades derivadas de la automatización. La aplicación efectiva de los derechos exige interpretar sus contenidos frente a nuevas capacidades de procesamiento, predicción y clasificación. Esta adaptación debe preservar la centralidad de la persona. El desarrollo del constitucionalismo digital ecuatoriano requiere, por tanto, integrar garantías sustantivas y procedimentales que permitan limitar tanto el poder tecnológico público como el privado.

Las decisiones automatizadas requieren garantías jurídicas compatibles con el debido proceso, la motivación, la transparencia y la posibilidad efectiva de revisión humana. No resulta suficiente que un sistema produzca decisiones técnicamente eficientes cuando sus criterios permanecen inaccesibles para quienes reciben sus consecuencias. La explicabilidad debe relacionarse con la capacidad real de comprender, cuestionar y controvertir resultados automatizados. Esta exigencia adquiere mayor intensidad cuando las decisiones afectan derechos, acceso a servicios públicos,

relaciones laborales, oportunidades económicas o cualquier esfera relevante de la vida personal.

La discriminación algorítmica evidencia que la aparente neutralidad tecnológica puede coexistir con resultados jurídicamente incompatibles con el principio de igualdad. Los sistemas automatizados procesan datos procedentes de realidades sociales donde existen desigualdades, patrones históricos y clasificaciones capaces de trasladarse hacia modelos predictivos. La respuesta jurídica debe atender tanto al diseño como a los resultados. Evaluaciones de impacto, auditorías y mecanismos de reclamación permiten identificar tratamientos diferenciados injustificados y establecer responsabilidades cuando una decisión automatizada lesiona derechos constitucionalmente protegidos.

La protección de datos personales constituye uno de los pilares del Derecho Digital ecuatoriano porque conecta autonomía individual, privacidad y control sobre la circulación de información. El consentimiento conserva relevancia, pero resulta insuficiente ante tratamientos masivos, perfilamiento e inferencias algorítmicas difíciles de anticipar por el titular. La legitimidad requiere transparencia, proporcionalidad y responsabilidad proactiva. En consecuencia, la protección efectiva demanda controles durante todo el ciclo de tratamiento, especialmente cuando intervienen datos biométricos, transferencias internacionales, servicios en la nube y decisiones automatizadas.

El análisis de identidad digital, desconexión laboral, derecho al olvido, neuroderechos e integridad informacional demuestra que la transformación tecnológica amplía las formas mediante las cuales puede afectarse la personalidad. Deepfakes, clonación de voz y procesamiento de datos neuronales comprometen dimensiones vinculadas con identidad, imagen, autonomía y dignidad. Algunas respuestas pueden construirse desde derechos existentes. Otras requieren desarrollo normativo específico. La evolución del ordenamiento deberá evitar una

proliferación meramente nominal de derechos y concentrarse en garantías exigibles, procedimientos accesibles y remedios efectivos.

La responsabilidad jurídica por daños asociados con inteligencia artificial demanda superar explicaciones centradas exclusivamente en la actuación inmediata del sistema tecnológico. En el funcionamiento de estas herramientas participan desarrolladores, proveedores, implementadores, responsables del tratamiento y entidades que adoptan decisiones apoyadas en resultados automatizados. La autonomía técnica no elimina la responsabilidad humana o institucional. Por ello, la imputación deberá considerar control, previsibilidad, deberes de diligencia, riesgos generados y capacidad de prevención, distinguiendo adecuadamente las dimensiones civil, administrativa, penal y vinculada con protección de datos.

La investigación permite sostener que Ecuador necesita avanzar hacia una gobernanza de inteligencia artificial basada en riesgos, derechos y responsabilidades diferenciadas. Una regulación uniforme resultaría insuficiente frente a sistemas cuyos efectos varían considerablemente según su finalidad y ámbito de utilización. Las aplicaciones de mayor impacto requieren obligaciones reforzadas de documentación, trazabilidad, evaluación y supervisión. Auditorías algorítmicas, certificaciones y espacios controlados de experimentación pueden contribuir a este propósito, siempre que permanezcan vinculados con garantías jurídicas y mecanismos institucionales de rendición de cuentas.

La construcción de un Derecho Digital ecuatoriano requiere también coordinación entre autoridades administrativas, órganos judiciales, organismos de protección de datos y entidades responsables de políticas tecnológicas. La fragmentación institucional puede producir vacíos de tutela, duplicidad de competencias y respuestas contradictorias frente a fenómenos que atraviesan distintas ramas jurídicas. Una arquitectura regulatoria coherente necesita competencias definidas y procedimientos de

cooperación. También requiere capacidad técnica. La especialización institucional debe acompañarse de mecanismos de revisión judicial capaces de garantizar derechos ante decisiones tecnológicas complejas.

En conjunto, el estudio permite afirmar que innovación y protección de derechos no constituyen objetivos necesariamente contrapuestos. El problema jurídico reside en establecer condiciones bajo las cuales el desarrollo tecnológico pueda integrarse al orden democrático sin debilitar dignidad, autonomía, igualdad y seguridad jurídica. Ecuador dispone de bases constitucionales y normativas relevantes, aunque persisten espacios que requieren articulación legislativa e institucional. El desarrollo futuro de un estatuto de derechos digitales e inteligencia artificial deberá mantener a la persona como referencia normativa frente a toda transformación tecnológica.

Referencias Bibliográficas

- Al-Dulaimi, A. O. M. (2025/2026). Legal responsibility for errors caused by artificial intelligence (AI) in the public sector. *International Journal of Law and Management*, 68(4), 695–. <https://doi.org/10.1108/IJLMA-08-2024-0295>
- Ameen, K. S. (2026). Judicial review of algorithmic administrative systems: Legality, fairness, and accountability. *Frontiers in Artificial Intelligence*. <https://doi.org/10.3389/frai.2026.1802986>
- Asamblea Constituyente del Ecuador. (2008). *Constitución de la República del Ecuador* [versión reformada]. Registro Oficial No. 449. Asamblea Nacional del Ecuador
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Suplemento del Registro Oficial No. 459, 26 de mayo de 2021. Texto de la Ley Orgánica de Protección de Datos Personales
- Asamblea Nacional del Ecuador. (2023). *Ley Orgánica para la Transformación Digital y Audiovisual*. Tercer Suplemento del Registro Oficial No. 245, 7 de febrero de 2023. Texto de la Ley Orgánica para la Transformación Digital y Audiovisual
- Asamblea Nacional del Ecuador. (2017/2026). *Código Orgánico Administrativo*. Registro Oficial, Segundo Suplemento No. 31 [edición actualizada]. Defensoría Pública del Ecuador
- Avbelj, M. (2024). Reconceptualizing constitutionalism in the AI-run algorithmic society. *German Law Journal*. Artículo en Cambridge Core
- Ballanca, E. (2025). Between ethics and algorithms: Protecting rights in the digital era. *Journal of Modern Science*, 64(4), 387–402. <https://doi.org/10.13166/jms/215775>
- Blurred realities: Legal strategies for the deepfake era. (2026). <https://doi.org/10.1177/1023263X261433380>
- Brogle, K., et al. (2025). Context-specific certification of AI systems: A pilot in the healthcare domain. *AI and Ethics*. <https://doi.org/10.1007/s43681-025-00720-w>
- Español, A. G. (2025). Regulatory sandboxes for AI in the majority world: A learning-centric approach to legal adaptation. *Cambridge Forum on AI: Law and Governance*. Artículo en Cambridge Core

- Fahey, E. (2023). Does the EU's digital sovereignty promote localisation in its model of data protection? *European Papers*. Artículo en *European Papers*
- Friedewald, M., et al. (2021). Data protection impact assessments in practice. En *Privacy and identity management*. Springer. https://doi.org/10.1007/978-3-030-95484-0_25
- Frosio, G. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, 29, 31–77. <https://doi.org/10.1111/eulj.12475>
- García Cáceres, D. V. (2025). *Digital sovereignty in the cloud and international law*. Universidad Central del Ecuador. Repositorio académico de la Universidad Central del Ecuador
- Gonzalez-Mohino, M., Rodriguez-Domenech, M. Á., Callejas-Albiñana, A. I., et al. (2023). Empowering critical thinking: The role of digital tools in citizen participation. *Journal of New Approaches in Educational Research*, 12, 258–275. <https://doi.org/10.7821/naer.2023.7.1385>
- Hogenhout, L., & Wangmo, R. (2025). *Protecting persona biometric data: The case of facial privacy*. arXiv. Preprint en arXiv
- Izquierdo-Rodas, W. E. (2026). Personal data protection and cybersecurity: Regulation, risks, and safeguards in the digital era. *Tribunal*. <https://doi.org/10.51247/tj.v3i2.977>
- Kasirzadeh, A., & Clifford, D. (2021). *Fairness and data protection impact assessments*. arXiv. Preprint en arXiv
- Kelly-Lyth, A. (2023). Algorithmic discrimination at work. *European Labour Law Journal*, 14(2), 152–171. <https://doi.org/10.1177/20319525231167300>
- Kiriak, O. V. (2021). The right to be forgotten: Emerging legal issues. *Review of European and Comparative Law*. <https://doi.org/10.31743/recl.12432>
- Lee, J.-A., & Sun, X. (2026). *Vocal identity under siege by AI voice cloning technologies*. arXiv. Preprint en arXiv
- Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2023). *Acuerdo Nro. MINTEL-MINTEL-2023-0019*. Suplemento del Registro Oficial No. 448, 30 de noviembre de 2023.
- Ministerio del Trabajo del Ecuador. (2022). *Acuerdo Ministerial Nro. MDT-2022-237: Directrices que regulan el contrato de teletrabajo y lineamientos del derecho de desconexión laboral*. Biblioteca normativa del Ministerio del Trabajo

- Moreira, A. (2026). Neurorights: Comparing some perspectives on legal reform and regulatory pathways. *Frontiers in Human Neuroscience*. <https://doi.org/10.3389/fnhum.2026.1873948>
- Mühlhoff, R. (2024). Predictive analytics and the collective dimensions of data protection. *International Review of Law, Computers & Technology*. <https://doi.org/10.1080/17579961.2024.2313794>
- Neubauer, A., Wynn, M. G., & Bown, G. R. (2026). AI, authorship, copyright, and human originality. *Encyclopedia*, 6(1), 9, 1–16. <https://doi.org/10.3390/encyclopedia6010009>
- Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of New Approaches in Educational Research*. <https://doi.org/10.7821/naer.2021.1.616>
- Presidencia de la República del Ecuador. (2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales* (Decreto Ejecutivo No. 904). Ministerio de Telecomunicaciones y de la Sociedad de la Información
- Presidencia de la República del Ecuador. (2023). *Reglamento General a la Ley Orgánica para la Transformación Digital y Audiovisual*. Texto del Reglamento General
- Quintais. (2025). Generative AI, copyright and the AI Act. *Computer Law & Security Review*, 56, 106107. <https://doi.org/10.1016/j.clsr.2025.106107>
- Rangone, N. (2025). Risks without rights? The EU AI Act's approach to AI in law and rulemaking. *European Journal of Risk Regulation*. Artículo en Cambridge Core
- Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework for safeguarding fundamental rights. *Computer Law & Security Review*. Artículo en ScienceDirect
- Rudolf, G., & Kovač, P. (2024). The role of automated decision-making in modern administrative law: Challenges and data protection implications. *Central European Public Administration Review*, 22(2), 83–108. <https://doi.org/10.17573/cepar.2024.2.04>
- Santos, C., Nouwens, M., Toth, M., Bielova, N., & Roca, V. (2021). Consent management platforms under the GDPR: Processors and/or controllers? *Proceedings on Privacy Enhancing Technologies*. Versión disponible en arXiv
- Sourdin, T. (2025). AI governance: A comparative approach. *German Law Journal*. Artículo en Cambridge Core
- Vardanyan, L., Hamul'ák, O., & Kocharyan, H. (2024). Fragmented identities: Legal challenges of digital identity, integrity, and

- informational self-determination. *European Studies*, 11(1), 105–121. <https://doi.org/10.2478/eustu-2024-0005>
- Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, 11, 1121. <https://doi.org/10.1057/s41599-024-03560-x>
- Zhao, Y. (2025). The alignment of values: Embedding human dignity in algorithmic governance. *International Journal of Digital Law and Governance*. <https://doi.org/10.1515/ijdlg-2025-0006>

Advertencia jurídica

El contenido de esta obra tiene fines académicos y profesionales. Las disposiciones, los procedimientos y los criterios examinados corresponden al marco normativo considerado durante su elaboración y pueden ser objeto de reformas, derogaciones o interpretaciones posteriores. En consecuencia, la información presentada no sustituye el análisis jurídico particular que deba efectuarse frente a cada situación concreta.



Red de Investigación
Científica y Desarrollo
Tecnológico **Del Pacífico**

Una guía esencial para comprender
el impacto jurídico de la transformación digital
y construir un futuro tecnológico con
derechos, ética y seguridad para todas las personas.


EDITORIAL
SAGA

ISBN: 978-9907-803-63-1



9 789907 803631