



**UNIVERSIDAD TECNOLÓGICA
INDOAMÉRICA
FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO**

TEMA:

**LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR: UN
ANÁLISIS DESDE LA CONSTITUCIONALIZACIÓN DIGITAL**

Trabajo de Integración Curricular previo a la obtención del título de Derecho

Autor(a)

Lizeth Carolina Rojas Lombeida

Tutor(a)

Dr. Marcelo Giovanni Galárraga
Carvajal

QUITO- ECUADOR
2026

**AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA,
REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA
DEL TRABAJO DE INTEGRACIÓN CURRICULAR**

Yo, Lizeth Carolina Rojas Lombeida, declaro ser autor del Trabajo de Integración Curricular con el nombre **“La protección de datos personales en ecuador: un análisis desde la constitucionalización digital.”**, como requisito para optar al grado de abogada y autorizo al Sistema de Bibliotecas de la Universidad Tecnológica Indoamérica, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDI-UTI).

Los usuarios del RDI-UTI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. La Universidad Tecnológica Indoamérica no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los Derechos de Autor, Morales y Patrimoniales, sobre esta obra, serán compartidos entre mi persona y la Universidad Tecnológica Indoamérica, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.

Para constancia de esta autorización, en la ciudad de Quito, a los 05 días del mes de marzo de 2026, firmo conforme:

Autor: Lizeth Carolina Rojas Lombeida

Firma: 

Número de Cédula: 1726369703

Dirección: Pichincha, Quito, Ponciano, Ponciano.

Correo Electrónico: lrojas.00@outlook.com

Teléfono: 0985747691

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Integración Curricular “LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR: UN ANÁLISIS DESDE LA CONSTITUCIONALIZACIÓN DIGITAL.” presentado por Lizeth Carolina Rojas Lombeida para optar por el Título de abogada

CERTIFICO

Que dicho Trabajo de Integración Curricular ha sido revisado en todas sus partes y considero que reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte los lectores que se designe.

Quito, 05 de marzo del 2026

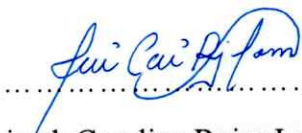


Dr. Marcelo Giovanni Galárraga Carvajal

DECLARACIÓN DE AUTENTICIDAD

Quien suscribe, declaro que los contenidos y los resultados obtenidos en el presente Trabajo de Integración Curricular, como requerimiento previo para la obtención del Título de Abogada, son absolutamente originales, auténticos y personales y de exclusiva responsabilidad legal y académica del autor

Quito, 05 de marzo del 2026



.....

Lizeth Carolina Rojas Lombeida
1726369703

APROBACIÓN DE LECTORES

El Trabajo de Integración Curricular ha sido revisado, aprobado y autorizada su impresión y empastado, sobre el Tema "LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR: UN ANÁLISIS DESDE LA CONSTITUCIONALIZACIÓN DIGITAL".
Previo a la obtención del Título de abogada, reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la sustentación del Trabajo de Integración Curricular.

Quito, 05 de marzo de 2026



.....
MSc. Erlin Ricardo Estrada Murillo
LECTOR



.....
MSc. Marcos Alexander Ortiz Muñoz
LECTOR

DEDICATORIA

A mis padres,
por ser el pilar firme sobre el que he construido cada uno de mis sueños.
Gracias por su amor incondicional, por su esfuerzo silencioso y por enseñarme, con su ejemplo, el valor de la perseverancia, la honestidad y la fe.

Este logro no es solo mío, es el reflejo de cada sacrificio suyo, de cada palabra de aliento en los momentos difíciles y de cada abrazo que me dio fuerzas para continuar.

Con profunda gratitud y amor eterno, este trabajo está dedicado a ustedes.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Dra. Clara Romero, quien fue mi guía durante todo el proceso del octavo semestre. Su paciencia, dedicación y compromiso académico fueron fundamentales para que pudiera desarrollar este trabajo con claridad y rigor. Gracias por inspirarme a dar siempre lo mejor de mí y por acompañarme en cada paso de este camino.

Agradezco profundamente al Dr. Marcelo Galarraga, mi tutor, por su orientación experta, sus valiosos consejos y su constante apoyo. Su guía ha sido esencial para fortalecer mis ideas y lograr que este proyecto alcance el nivel académico que hoy presento.

A ambos, mi gratitud y respeto eterno por su dedicación, generosidad y profesionalismo.

ÍNDICE DE CONTENIDOS

PORTADA.....	i
AUTORIZACIÓN PARA EL REPOSITORIO DIGITAL	ii
APROBACIÓN DEL TUTOR	iii
INTRODUCCIÓN.....	2
1.LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL DE CUARTA GENERACIÓN	3
2.DIFERENCIAS ENTRE PRIVACIDAD, INTIMIDAD Y PROTECCIÓN DE DATOS...	5
3.MARCO CONSTITUCIONAL ECUATORIANO SOBRE PROTECCIÓN DE DATOS PERSONALES.....	6
4.EL HÁBEAS DATA COMO GARANTÍA DE LOS DERECHOS DIGITALES	8
5.ANÁLISIS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES..	9
6.JURISPRUDENCIA CONSTITUCIONAL ECUATORIANA SOBRE DATOS PERSONALES.....	12
7.LA CONSTITUCIONALIZACIÓN DIGITAL Y SU INFLUENCIA EN EL SISTEMA JURÍDICO ECUATORIANO	14
8.PROTECCIÓN DE DATOS PERSONALES FRENTE A LA INTELIGENCIA ARTIFICIAL.....	15
9.RESPONSABILIDAD DEL ESTADO EN EL TRATAMIENTO DE DATOS PERSONALES.....	17
CONCLUSIONES.....	18
BIBLIOGRAFÍA:	20

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA
FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

**TEMA: LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR: UN ANÁLISIS
DESDE LA CONSTITUCIONALIZACIÓN DIGITAL**

AUTORA: Lizeth Carolina Rojas Lombeida

TUTOR: Dr. Marcelo Giovanni Galárraga
Carvajal

Resumen

La acelerada transición hacia ecosistemas digitales ha generado un escenario en el que la protección de datos personales adquiere un rol central dentro del sistema jurídico ecuatoriano. La constitucionalización digital entendida como el proceso mediante el cual los principios constitucionales se proyectan hacia los entornos tecnológicos ha fortalecido el reconocimiento de los datos personales como un derecho fundamental de cuarta generación, impulsando la necesidad de garantizar su ejercicio efectivo frente a nuevas dinámicas sociales, económicas y tecnológicas. En este contexto, el presente artículo examina de manera crítica la evolución normativa y jurisprudencial del Ecuador respecto de la protección de datos personales, partiendo de la distinción conceptual entre privacidad, intimidad y autodeterminación informativa, se analiza el marco constitucional de 2008 y el desarrollo del hábeas data como garantía jurisdiccional que protege el acceso, rectificación y actualización de información personal. Del mismo modo, se estudia la Ley Orgánica de Protección de Datos Personales de 2021 y su reglamentación, evaluando sus alcances, principios, limitaciones y mecanismos institucionales de control. El artículo aborda los desafíos emergentes que plantea la inteligencia artificial para el tratamiento responsable de información personal, así como los deberes de diligencia reforzada del Estado frente a vulneraciones derivadas del uso indebido, inseguro o desproporcionado de datos. El objetivo central es demostrar cómo la constitucionalización digital reconfigura la interpretación de derechos y obligaciones, y exige la consolidación de un modelo garantista que responda a los riesgos actuales de la sociedad digital.

Palabras clave: Constitucionalización digital; Datos personales; Derechos digitales; Hábeas data; Protección de datos.

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA
FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

**TEMA: PERSONAL DATA PROTECTION IN ECUADOR: AN ANALYSIS
FROM DIGITAL CONSTITUTIONALIZATION**

AUTORA: Lizeth Carolina Rojas Lombeida

TUTOR: Dr. Marcelo Giovanni Galárraga
Carvajal

Abstract:

The accelerated transition toward digital ecosystems has created a scenario in which personal data protection plays a central role within the Ecuadorian legal system. Digital constitutionalization understood as the process through which constitutional principles are projected into technological environments has strengthened the recognition of personal data as a fourth-generation fundamental right, reinforcing the need to guarantee its effective exercise in the face of new social, economic, and technological dynamics. This article critically examines the normative and jurisprudential evolution of personal data protection in Ecuador, beginning with the conceptual distinction between privacy, intimacy, and informational self-determination. It analyzes the 2008 Constitution and the development of habeas data as a jurisdictional guarantee that protects access, rectification, and updating of personal information. Likewise, it studies the 2021 Organic Law on Personal Data Protection and its regulations, evaluating their scope, principles, limitations, and institutional control mechanisms. Finally, the article addresses emerging challenges posed by artificial intelligence for the responsible processing of personal information, as well as the State's heightened duties of diligence in cases of improper, unsafe, or disproportionate data use. The central objective is to demonstrate how digital constitutionalization reshapes the interpretation of rights and obligations and demands the consolidation of a guarantee-based model capable of responding to the current risks of the digital society.

Keywords: Digital constitutionalization; Digital rights; Habeas data; Personal data; Data protection.

La protección de datos personales en Ecuador: un análisis desde la constitucionalización digital

Personal Data Protection in Ecuador: An Analysis from Digital Constitutionalization

Lizeth Carolina Rojas Lombeida 1[0009-0009-6948-916X], Marcelo Giovanni Galárraga Carvajal 2[0000-0003-2205-2875]

1Facultad de Jurisprudencia y Ciencias Políticas, Carrera Derecho, Universidad Tecnológica Indoamérica, 170103, Quito, Ecuador

2Jurisprudencia y Ciencias Políticas, Universidad Indoamérica, 170103, Quito, Ecuador

lrojas4@indoamerica.edu.ec,marcelogalarraga@uti.edu.ec

Resumen

La acelerada transición hacia ecosistemas digitales ha generado un escenario en el que la protección de datos personales adquiere un rol central dentro del sistema jurídico ecuatoriano. La constitucionalización digital entendida como el proceso mediante el cual los principios constitucionales se proyectan hacia los entornos tecnológicos ha fortalecido el reconocimiento de los datos personales como un derecho fundamental de cuarta generación, impulsando la necesidad de garantizar su ejercicio efectivo frente a nuevas dinámicas sociales, económicas y tecnológicas. En este contexto, el presente artículo examina de manera crítica la evolución normativa y jurisprudencial del Ecuador respecto de la protección de datos personales, partiendo de la distinción conceptual entre privacidad, intimidad y autodeterminación informativa, se analiza el marco constitucional de 2008 y el desarrollo del hábeas data como garantía jurisdiccional que protege el acceso, rectificación y actualización de información personal. Del mismo modo, se estudia la Ley Orgánica de Protección de Datos Personales de 2021 y su reglamentación, evaluando sus alcances, principios, limitaciones y mecanismos institucionales de control. El artículo aborda los desafíos emergentes que plantea la inteligencia artificial para el tratamiento responsable de información personal, así como los deberes de diligencia reforzada del Estado frente a vulneraciones derivadas del uso indebido, inseguro o desproporcionado de datos. El objetivo central es demostrar cómo la constitucionalización digital reconfigura la interpretación de derechos y obligaciones, y exige la consolidación de un modelo garantista que responda a los riesgos actuales de la sociedad digital.

Palabras clave: Constitucionalización digital; Datos personales; Derechos digitales; Hábeas data; Protección de datos.

Abstract

The accelerated transition toward digital ecosystems has created a scenario in which personal data protection plays a central role within the Ecuadorian legal system. Digital constitutionalization understood as the process through which constitutional principles are projected into technological environments has strengthened the recognition of personal data as a fourth-generation fundamental right, reinforcing the need to guarantee its effective exercise in the face of new social, economic, and technological dynamics. This article critically examines the normative and jurisprudential evolution of personal data protection in Ecuador, beginning with the conceptual distinction between privacy, intimacy, and informational self-determination. It analyzes the 2008 Constitution and the development of habeas data as a jurisdictional guarantee that protects access, rectification, and updating of personal information. Likewise, it studies the 2021 Organic Law on Personal Data Protection and its regulations, evaluating their scope, principles, limitations, and institutional control mechanisms. Finally, the article addresses emerging challenges posed by artificial intelligence for the responsible processing of personal information, as well as the State's heightened duties of diligence in cases of improper, unsafe, or disproportionate data use. The central objective is to demonstrate how digital constitutionalization reshapes the interpretation of rights and obligations and demands the consolidation of a guarantee-based model capable of responding to the current risks of the digital society.

Keywords: Digital constitutionalization; Digital rights; Habeas data; Personal data; Data protection.

Introducción

La revolución tecnológica de las últimas décadas ha modificado de manera profunda la forma en que las personas se relacionan, interactúan, acceden a servicios y participan en la vida social. En este nuevo entorno digitalizado, la información personal se ha convertido en un recurso estratégico con alto valor económico, político y social. La masificación del uso de plataformas digitales, el despliegue de tecnologías basadas en inteligencia artificial y la recolección permanente de datos han provocado que la protección de datos personales se configure como uno de los ejes centrales en la agenda jurídica contemporánea. Para el caso ecuatoriano, este fenómeno adquiere particular relevancia debido al proceso de constitucionalización digital, mediante el cual los principios y derechos reconocidos en la Constitución se adaptan y se proyectan hacia los entornos tecnológicos donde hoy se desarrollan múltiples interacciones humanas. Reconocer los datos personales como un derecho fundamental de cuarta generación implica comprender que su protección no se limita al ámbito privado, sino que se articula con valores esenciales como la dignidad humana, la autonomía individual, el libre desarrollo de la personalidad y la autodeterminación informativa.

En este contexto, el Ecuador ha experimentado avances significativos tanto a nivel normativo como jurisprudencial, con la incorporación de garantías como el hábeas data, la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021 y la creciente intervención de la Corte Constitucional en casos relacionados con vulneraciones a derechos digitales. No obstante, la consolidación de un sistema de protección de datos verdaderamente efectivo enfrenta desafíos profundos, especialmente frente al poder de las grandes plataformas tecnológicas, la circulación transfronteriza de información, el uso opaco de algoritmos y la asimetría existente entre quienes generan datos y quienes los procesan. (LOPDP, 2021).

En consecuencia, el presente artículo tiene como objetivo analizar la protección de los datos personales en el Ecuador desde la perspectiva de la constitucionalización digital, con el fin de examinar su reconocimiento como derecho fundamental de cuarta generación, su desarrollo en el marco constitucional y legal, el rol del hábeas data y de la jurisprudencia constitucional, así como los desafíos que plantea el uso de tecnologías emergentes, en particular la inteligencia artificial, y la responsabilidad del Estado en el tratamiento de la información personal.

Desde esta óptica, el estudio de la protección de datos permite evidenciar tensiones normativas, vacíos regulatorios y riesgos emergentes, así como la necesidad de adoptar un enfoque garantista que coloque a la dignidad humana en el centro de la regulación tecnológica. En este contexto, el problema jurídico que orienta la presente investigación puede formularse en los siguientes términos: ¿De qué manera el proceso de constitucionalización digital ha reconfigurado el alcance del derecho a la protección de datos personales en el Ecuador y cuáles son sus implicaciones para el sector público y privado en el tratamiento de información personal? La tesis que se sostiene es que la constitucionalización digital ha transformado este derecho en una categoría fundamental autónoma con eficacia directa, ampliando sus garantías jurisdiccionales e imponiendo obligaciones reforzadas tanto al Estado como a los particulares. Metodológicamente, el estudio se desarrolla bajo un enfoque dogmático-jurídico, mediante el análisis sistemático del marco constitucional ecuatoriano, de la Ley Orgánica de Protección de Datos Personales y de la jurisprudencia reciente de la Corte Constitucional, a fin de evaluar la evolución normativa e interpretativa del derecho en el contexto de la sociedad digital.

1. La protección de datos como derecho fundamental de cuarta generación

El reconocimiento de la protección de datos personales como derecho fundamental ha experimentado una evolución progresiva en el derecho comparado y en el sistema constitucional ecuatoriano. Desde una perspectiva doctrinaria, algunos sectores de la teoría de los derechos fundamentales han clasificado la protección de datos personales como un derecho de “cuarta generación”, en tanto surge en respuesta a los desafíos tecnológicos propios de la sociedad de la información y se vincula con fenómenos como la digitalización, la automatización y el tratamiento masivo de datos. No obstante, esta categorización no es pacífica, pues la teoría de las generaciones de derechos ha sido objeto de críticas por su carácter evolutivo lineal y por la dificultad de encuadrar derechos complejos dentro de compartimentos rígidos.

En el contexto ecuatoriano, más que adoptar de manera categórica la noción de cuarta generación, resulta más preciso afirmar que la protección de datos personales constituye una manifestación contemporánea de los derechos fundamentales clásicos, particularmente del derecho a la intimidad, a la dignidad y a la autodeterminación informativa, cuya expansión responde al proceso de constitucionalización digital (Rodotà, 2003; CRE, 2008). En este sentido, su relevancia no deriva tanto de su ubicación generacional como de su reconocimiento constitucional expreso y de su eficacia directa dentro del modelo de Estado constitucional de derechos y justicia. Su importancia radica en la necesidad de proteger a las personas frente al poder creciente que adquieren tanto el Estado como los actores privados en contextos marcados por el big data, la automatización y la inteligencia artificial (Piñar, et al., 2016).

En el ámbito ecuatoriano, la Dirección Nacional de Registros Públicos ha señalado que la protección de datos personales posee reconocimiento constitucional, lo

que impone al Estado la obligación de establecer mecanismos eficaces para su garantía. Este reconocimiento no solo amplía el catálogo de derechos fundamentales, sino que redefine la relación entre el individuo y las instituciones públicas y privadas, al vincularse directamente con la autodeterminación informativa. DINARP, (2021).

El carácter autónomo del derecho a la protección de datos personales encuentra sustento directo en el artículo 66 numeral 19 de la Constitución de la República del Ecuador, que reconoce expresamente el derecho de las personas a la protección de datos de carácter personal, incluyendo el acceso, rectificación, eliminación y oposición frente a su tratamiento. (CRE, 2008). Esta formulación normativa no lo subsume dentro del derecho a la intimidad, sino que lo configura como una garantía específica vinculada al control sobre la información personal, evidenciando una voluntad constitucional de dotarlo de identidad propia dentro del catálogo de derechos fundamentales.

Desde una perspectiva teórica, la protección de datos se distingue del derecho a la intimidad en cuanto no se limita a resguardar ámbitos reservados de la vida privada, sino que otorga al titular un poder de disposición sobre el flujo, circulación y tratamiento de su información, incluso cuando esta no sea estrictamente íntima. Mientras la intimidad protege un espacio frente a injerencias externas, la protección de datos regula las condiciones bajo las cuales terceros (públicos o privados) pueden tratar información personal, exigiendo licitud, finalidad, proporcionalidad y responsabilidad activa. En este sentido, su autonomía no deriva únicamente de su reconocimiento constitucional expreso, sino de su contenido material diferenciado y de su función estructural dentro del Estado constitucional de derechos y justicia.

Esta se entiende como la facultad de cada persona para decidir sobre la recolección, uso, tratamiento y circulación de su información personal, noción que, aunque desarrollada inicialmente por el Tribunal Constitucional alemán, ha sido incorporada por diversos ordenamientos jurídicos, incluido el ecuatoriano, como un elemento esencial para la protección de la dignidad humana en entornos digitales. En este sentido, (Ordóñez, 2021) sostiene que la protección de datos personales debe concebirse como un derecho autónomo que trasciende la esfera estrictamente privada, al incidir en dimensiones como la libertad, la identidad, la seguridad y el control sobre la información personal.

La vulneración de este derecho puede generar impactos directos en el ejercicio de otros derechos fundamentales, tales como la intimidad, la igualdad, la no discriminación y la participación democrática, especialmente en contextos de interacción digital y acceso a servicios. Asimismo, (Hernández, et al., 2025) advierten que la expansión de la inteligencia artificial y la digitalización intensifican los riesgos asociados al tratamiento de datos personales, debido a prácticas como la recopilación masiva de información, la opacidad de los sistemas algorítmicos y la toma de decisiones automatizadas sin supervisión humana adecuada. Estas dinámicas pueden derivar en afectaciones graves a los derechos fundamentales si no existen marcos normativos sólidos y autoridades de control independientes.

En este contexto, el carácter de derecho de cuarta generación implica que la protección de datos personales no es estática, sino que exige una adaptación constante frente a los avances tecnológicos y los riesgos emergentes. El Estado ecuatoriano enfrenta el deber de garantizar un sistema normativo coherente y actualizado, acompañado de políticas públicas, instituciones especializadas y mecanismos efectivos de reparación. Paralelamente, resulta necesario fomentar una cultura de protección de datos que

promueva el manejo responsable de la información personal. De este modo, la protección de datos personales se consolida como un pilar del constitucionalismo contemporáneo en Ecuador, orientado a responder de forma garantista a los desafíos propios de la sociedad digital.

2. Diferencias entre privacidad, intimidad y protección de datos

Desde la teoría constitucional contemporánea, la doctrina coincide en que la privacidad, la intimidad y la protección de datos personales son conceptos jurídicos distintos, aunque estrechamente relacionados, cuya diferenciación resulta esencial para una adecuada tutela de los derechos fundamentales, tal como lo señalan (Ávila 2019; Muñoa 2022). Si bien estos términos han sido utilizados en ocasiones como sinónimos, su distinción permite delimitar con mayor precisión el contenido y alcance de cada derecho en la vida de las personas.

La privacidad ha sido tradicionalmente entendida como el ámbito reservado de la vida de una persona frente a terceros, e implica la facultad de controlar qué información personal se comparte y con quién. Desde una perspectiva jurídica, este derecho protege aspectos como relaciones familiares, comportamientos cotidianos, preferencias, hábitos o actividades que no deben ser expuestos sin autorización. La privacidad presenta una dimensión negativa, vinculada al derecho a no ser objeto de injerencias, y una dimensión positiva, relacionada con la posibilidad de decidir activamente qué elementos de la vida personal pueden hacerse públicos.

La intimidad, en cambio, constituye una esfera más profunda y restringida que la privacidad, al estar vinculada a sentimientos, creencias, emociones, orientación sexual, convicciones morales y otros aspectos profundamente personales. Como sostiene (Ávila 2019), la intimidad forma parte del núcleo esencial de la persona, razón por la cual su protección debe ser especialmente rigurosa, dado que su vulneración afecta de manera directa la dignidad humana. En este sentido, la intimidad puede entenderse como un círculo más reducido dentro del ámbito general de la privacidad.

Por su parte, la protección de datos personales se configura como un derecho autónomo, cuyo objeto no es el contenido de la información, sino el tratamiento que se realiza sobre cualquier dato personal, sea o no de carácter privado o íntimo. (LOPD, art. 4, 2018). Este derecho regula las operaciones de recolección, almacenamiento, organización, procesamiento, transmisión y eliminación de información relativa a una persona identificada o identificable. Así, incluso datos que no pertenecen a la esfera íntima, como una dirección domiciliaria o un número telefónico, se encuentran protegidos por las normas de protección de datos.

Según Muñoa, et al., (2022), la protección de datos personales exige el respeto de principios como la licitud del tratamiento, la finalidad específica, la minimización, la transparencia, la seguridad y la responsabilidad del responsable del tratamiento. La cuestión central, por tanto, no radica en si el dato es íntimo o privado, sino en si su tratamiento respeta los derechos fundamentales del titular.

Esta distinción cobra especial relevancia en el contexto digital actual, caracterizado por el uso masivo de redes sociales, aplicaciones móviles, sistemas de videovigilancia, reconocimiento facial y algoritmos predictivos, donde las fronteras entre información privada, íntima y pública se vuelven difusas. En muchos casos, las personas comparten datos personales sin plena conciencia de los riesgos asociados o del alcance

de su tratamiento. (Hidalgo, et al., 2023). Frente a este escenario, la protección de datos personales se consolida como un mecanismo esencial para evitar que la digitalización de la información vulnere la dignidad humana, el libre desarrollo de la personalidad o los derechos democráticos. En síntesis, mientras la privacidad y la intimidad protegen contenidos específicos de la vida personal, la protección de datos regula el tratamiento de toda información personal, lo que justifica su reconocimiento como un derecho autónomo dentro del constitucionalismo digital contemporáneo.

3. Marco constitucional ecuatoriano sobre protección de datos personales

El reconocimiento constitucional de la protección de datos personales en el Ecuador se inserta en el modelo de Estado constitucional de derechos y justicia consagrado en la Constitución de la República del Ecuador (2008), interpretación desarrollada por la doctrina nacional. La Constitución ecuatoriana constituye uno de los instrumentos normativos más avanzados de la región en materia de derechos digitales, al incorporar principios que reconocen la información personal como un bien jurídico protegido de manera autónoma y al establecer obligaciones claras tanto para el Estado como para quienes tratan datos de terceros. (CRE, 2008).

El artículo 66, numeral 19, reconoce el derecho de las personas a acceder, actualizar y rectificar la información que conste sobre ellas en archivos o bases de datos, sean públicos o privados. Esta disposición configura la base constitucional del derecho a la protección de datos personales, al garantizar no solo el acceso a la información, sino también el control sobre su uso y la prohibición de divulgar datos que afecten la honra u otros derechos fundamentales sin autorización. (CRE, 2008). De esta forma, se refuerza el principio de autodeterminación informativa como eje central del constitucionalismo digital. Asimismo, el artículo 92 incorpora el hábeas data como garantía constitucional destinada a proteger estos derechos, permitiendo a las personas conocer el uso que se hace de su información y exigir su rectificación o eliminación cuando sea errónea o cause afectaciones. (CRE, 2008) Esta garantía adquiere especial relevancia en un entorno digital caracterizado por el almacenamiento masivo de datos en sistemas automatizados y plataformas tecnológicas, tanto públicas como privadas.

De manera complementaria, el artículo 18 reconoce el derecho a la protección de la correspondencia y de las comunicaciones privadas, mientras que el artículo 66, numeral 20, prohíbe la interceptación de datos sin orden judicial. Aunque tradicionalmente vinculadas a la intimidad y la privacidad, estas disposiciones constituyen pilares esenciales para la protección de datos personales frente a prácticas como la vigilancia masiva, el rastreo de actividades en línea o las interceptaciones ilegales. La Constitución refuerza este marco al disponer, en el artículo 85, que la formulación, ejecución y evaluación de políticas públicas deben garantizar el pleno ejercicio de los derechos fundamentales, incluidos aquellos relacionados con la información personal. (CRE, 2008). Esto implica que la protección de datos no es únicamente un derecho pasivo, sino también un deber activo del Estado, que debe desarrollar instituciones, políticas y procedimientos específicos para su efectividad. En este contexto, la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021 representa un avance significativo en la concreción de los mandatos constitucionales. (LOPD, 2021)

Hidalgo (2023), sostiene que el marco constitucional ecuatoriano adopta una perspectiva progresiva al reconocer la protección de datos como un componente esencial

de la vida digna, la libertad personal y la participación democrática. La Constitución establece un equilibrio entre la transparencia de la gestión pública y la necesidad de garantizar la confidencialidad y seguridad de los datos personales, especialmente en ámbitos sensibles como la salud, la educación, la justicia, la seguridad social y el sistema financiero. (CRE, 2008). En definitiva, la constitucionalización de la protección de datos personales se articula con un modelo de Estado garantista que sitúa al ser humano en el centro del ordenamiento jurídico. La Constitución no solo reconoce este derecho, sino que también habilita mecanismos para su exigibilidad, impone límites al uso estatal de la información y orienta la interpretación de la normativa infra constitucional y de la legislación especializada en materia de datos personales.

Desde una perspectiva sistemática, el reconocimiento constitucional del derecho a la protección de datos personales no puede entenderse como una disposición aislada dentro del texto constitucional, sino como parte de un entramado normativo que articula dignidad humana, supremacía constitucional y eficacia directa de los derechos fundamentales. El artículo 66 numeral 19 debe interpretarse en conexión con el modelo de Estado constitucional de derechos y justicia, lo que implica que su protección no depende exclusivamente del desarrollo legislativo posterior, sino que posee aplicabilidad inmediata frente a actuaciones tanto de autoridades públicas como de particulares.

En términos materiales, este derecho no se limita a impedir injerencias arbitrarias, sino que impone deberes positivos al Estado, tales como la creación de marcos regulatorios adecuados, autoridades de control independientes y mecanismos jurisdiccionales efectivos. Su dimensión objetiva proyecta efectos sobre todo el ordenamiento jurídico, condicionando la validez de políticas públicas, sistemas tecnológicos y prácticas empresariales que involucren tratamiento de datos personales. De este modo, la protección de datos personales opera como un límite estructural al ejercicio del poder en contextos de digitalización creciente.

Este desarrollo normativo evidencia que la constitucionalización digital no constituye una categoría teórica aislada, sino un proceso real de reinterpretación de los derechos fundamentales frente a la transformación tecnológica del Estado y de la sociedad, consolidando la protección de datos como manifestación directa del constitucionalismo contemporáneo.

4. El hábeas data como garantía de los derechos digitales

El hábeas data ha sido conceptualizado como una garantía jurisdiccional destinada a proteger la autodeterminación informativa de las personas, criterio sostenido tanto por la Corte Constitucional del Ecuador (2024) como por la doctrina especializada en derechos digitales, representada por Pérez (2024). El hábeas data es una garantía jurisdiccional que tiene como finalidad asegurar el derecho de toda persona a conocer, acceder, rectificar, actualizar y, cuando corresponda, suprimir información personal almacenada en archivos, registros o bases de datos de instituciones públicas o privadas.

En el contexto digital, esta garantía se convierte en una herramienta esencial para salvaguardar derechos frente al uso masivo e indiscriminado de datos personales. En Ecuador, la constitucionalización del hábeas data (artículo 92 de la Constitución) responde a la necesidad de dotar a las personas de un mecanismo rápido y eficaz para controlar su información en una sociedad marcada por la digitalización y por la centralidad de los datos en múltiples actividades económicas, administrativas y sociales.

(CRE, 2008). Pérez (2024) señala que, en el marco de la era digital, el hábeas data adquiere una dimensión reforzada, ya que permite vigilar no solo la existencia de datos, sino también la finalidad, licitud y proporcionalidad del tratamiento realizado.

La Corte Constitucional ha desarrollado jurisprudencia significativa sobre el alcance del hábeas data. En la Sentencia No. 151- 21-JD-24 (2024), la Corte determinó que el procesamiento de información personal sin autorización expresa del titular constituye una vulneración directa del derecho, incluso cuando la información no sea considerada sensible. Esta decisión reafirma que el consentimiento informado es un requisito indispensable para cualquier tratamiento de datos, y que su ausencia deriva en responsabilidad estatal o privada. Asimismo, la Corte ha enfatizado la importancia del principio de minimización de datos, estableciendo que ninguna entidad puede recolectar información más allá de lo estrictamente necesario. (CCE, 2024).

Desde una perspectiva técnico constitucional, la ratio decidendi de la Sentencia No. 151-21-JD-24 radica en el reconocimiento de que el consentimiento informado y el principio de minimización constituyen requisitos estructurales del tratamiento legítimo de datos personales, cuya inobservancia activa de manera directa la tutela del hábeas data. El criterio vinculante que se desprende del fallo establece que cualquier tratamiento sin autorización válida o que exceda la finalidad declarada configura una vulneración autónoma del derecho, independientemente de que se trate de datos sensibles o no.

En cambio, las referencias efectuadas por la Corte al contexto de expansión tecnológica y a los riesgos derivados de la digitalización masiva cumplen una función argumentativa complementaria, pero no constituyen el núcleo obligatorio de la decisión. Esta diferenciación permite identificar con claridad la regla jurisprudencial aplicable y fortalece la seguridad jurídica en la interpretación del alcance del hábeas data dentro del modelo constitucional ecuatoriano.

Las bases de datos no pueden utilizarse para fines distintos a los informados, y cualquier tratamiento adicional debe contar con una nueva autorización del titular. Esta interpretación fortalece la noción de autodeterminación informativa y evita prácticas que puedan resultar invasivas o discriminatorias. El hábeas data también se ha aplicado para corregir información errónea o desactualizada que afecta derechos fundamentales. En un entorno donde algoritmos y sistemas automatizados procesan millones de datos, la existencia de información incorrecta puede conducir a exclusiones, sanciones injustificadas, negativas de acceso a servicios o discriminación indirecta. (Hernández, 2025).

De allí que esta garantía sea indispensable para verificar la veracidad y exactitud de los datos que se manejan sobre una persona. El hábeas data constituye una pieza clave en la arquitectura del constitucionalismo digital ecuatoriano. (Hidalgo, 2023). Su función protectora se extiende a todos los ámbitos donde la información personal pueda ser recopilada o utilizada, convirtiéndose en un instrumento que equilibra las relaciones entre individuos, Estado y empresas tecnológicas. La ampliación de su alcance, especialmente en el contexto de la inteligencia artificial y la digitalización masiva, lo consolida como una garantía esencial para la defensa de los derechos digitales contemporáneos.

5. Análisis de la Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales (LOPD), aprobada en el Ecuador en 2021, constituye uno de los avances legislativos más relevantes dentro del

proceso de constitucionalización digital del país. Esta norma desarrolla el derecho a la autodeterminación informativa reconocido en la Constitución de 2008 y responde a la necesidad de establecer estándares claros para el tratamiento de datos personales en un entorno caracterizado por la circulación masiva, automatizada y permanente de información (LOPD, 2021). La ley se inspira en estándares internacionales y en modelos comparados de protección de datos, especialmente europeos, como lo reconoce la Asamblea Nacional del Ecuador (2021) y lo analiza Hidalgo (2023). La LOPDP se enmarca en una visión moderna que reconoce a los datos personales como un recurso estratégico y altamente sensible, capaz de incidir directamente en la dignidad y en el ejercicio de los derechos fundamentales. En este sentido, establece principios esenciales que orientan todo tratamiento de información, tales como la licitud, la finalidad, la proporcionalidad, la minimización, la calidad, la transparencia y la seguridad. Estos principios buscan evitar prácticas excesivas o arbitrarias y obligan a que el tratamiento de datos responda a causas legítimas claramente justificadas por el responsable.

Uno de los ejes centrales de la LOPDP es la regulación del consentimiento como base de legitimidad del tratamiento. La ley exige que este sea libre, específico, inequívoco e informado, garantizando que el titular conozca plenamente la finalidad para la cual se utilizan sus datos, asimismo, prohíbe que el consentimiento sea inferido u obtenido mediante mecanismos engañosos, cláusulas ambiguas o presiones indebidas, y establece la obligación de recabar un nuevo consentimiento cuando la finalidad del tratamiento sea modificada. De este modo, se refuerza el control permanente del titular sobre su información personal y se previene el uso abusivo de los datos. La ley introduce un régimen reforzado para el tratamiento de datos sensibles, tales como información biométrica, genética, de salud, orientación sexual, religión o convicciones políticas, debido a su especial potencial para generar discriminación o

afectaciones graves a la dignidad humana. En estos casos, la LOPDP adopta un enfoque precautorio, imponiendo mayores restricciones, medidas de seguridad más estrictas y limitaciones específicas sobre su recolección, uso y divulgación.

Otro aspecto fundamental es la obligación de implementar medidas de seguridad técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. La LOPDP establece que la seguridad no constituye una opción discrecional, sino un deber jurídico, cuyo incumplimiento puede generar responsabilidad administrativa, civil e incluso constitucional. Entre estas medidas se incluyen controles de acceso, protocolos internos, análisis de riesgos, auditorías y mecanismos de gestión de incidentes. (LOPD, 2021). Asimismo, la ley incorpora instrumentos preventivos como las evaluaciones de impacto en protección de datos, obligatorias cuando el tratamiento implica altos riesgos para los derechos de las personas o involucra datos sensibles. Estas evaluaciones permiten anticipar posibles afectaciones y adoptar medidas correctivas, lo cual resulta especialmente relevante frente al uso de tecnologías como el reconocimiento facial, la videovigilancia inteligente, los sistemas predictivos y la inteligencia artificial.

La transparencia constituye otro pilar estructural de la LOPDP, al exigir que los responsables informen de manera clara y accesible sobre la finalidad del tratamiento, la base legal, el tiempo de conservación y las posibles transferencias de datos. Esta obligación fortalece la confianza ciudadana y facilita el ejercicio de los derechos de acceso, rectificación y control sobre la información personal. En cuanto a los derechos de los titulares, la ley reconoce un catálogo amplio que incluye el acceso, rectificación, actualización, cancelación, oposición, portabilidad y suspensión del tratamiento. Estos

derechos permiten a las personas mantener un control efectivo sobre sus datos, especialmente frente a tratamientos automatizados, perfiles algorítmicos o fines comerciales potencialmente invasivos. De manera particular, la LOPDP regula las decisiones automatizadas, estableciendo que ninguna persona puede ser objeto de decisiones basadas exclusivamente en procesos automatizados que produzcan efectos jurídicos significativos sin intervención humana. (LOPDP, 2021)

La LOPDP crea la Superintendencia de Protección de Datos Personales como autoridad de control encargada de supervisar, regular y sancionar los tratamientos indebidos. Esta entidad cuenta con competencias para emitir directrices, investigar infracciones, imponer sanciones y ordenar la cesación de prácticas ilícitas, constituyéndose en una manifestación concreta del compromiso estatal con la protección efectiva de los datos personales. En conjunto, la LOPDP posiciona al Ecuador dentro de un modelo moderno de protección de datos, alineado con estándares internacionales y orientado a garantizar un equilibrio entre innovación tecnológica y respeto a los derechos fundamentales.

La Ley Orgánica de Protección de Datos Personales impone obligaciones jurídicas concretas y exigibles tanto al sector público como al privado, consolidando un modelo de responsabilidad activa en el tratamiento de información personal. No se trata únicamente de reconocer principios generales, sino de exigir la implementación de programas integrales de protección de datos que incluyan políticas internas, medidas técnicas y organizativas de seguridad, protocolos de gestión de incidentes y mecanismos eficaces para atender los derechos de los titulares. En el caso del sector público, estas obligaciones adquieren un carácter reforzado debido a la naturaleza sensible de la información que administra y a la posición de supremacía institucional que limita la libertad real del consentimiento ciudadano. En el ámbito privado, especialmente en sectores que operan plataformas digitales o sistemas de análisis masivo de datos, la ley prohíbe la recopilación indiscriminada y la reutilización de información sin consentimiento expreso, imponiendo estándares estrictos de licitud, finalidad y proporcionalidad.

El control del cumplimiento de estas obligaciones recae en la Superintendencia de Protección de Datos Personales, autoridad técnica especializada encargada de supervisar, fiscalizar y sancionar tratamientos indebidos. Su rol no se limita a la imposición de multas, sino que comprende funciones preventivas, regulatorias y pedagógicas orientadas a garantizar la efectividad material del derecho. No obstante, la eficacia del sistema dependerá de su autonomía institucional, recursos técnicos y capacidad real de fiscalización frente a entidades públicas y grandes actores económicos. De este modo, la protección de datos personales se consolida no solo como un mandato normativo, sino como un sistema estructurado de control que articula obligaciones, supervisión y responsabilidad jurídica.

No obstante, pese a su solidez normativa, la implementación efectiva de la LOPDP enfrenta desafíos estructurales que podrían limitar su impacto práctico. Entre ellos se encuentra la necesidad de fortalecer la capacidad técnica, presupuestaria y operativa de la Superintendencia de Protección de Datos Personales, cuya eficacia depende de su autonomía institucional y de su capacidad real para fiscalizar tanto a entidades públicas como a grandes actores privados que manejan volúmenes masivos de información.

De la misma manera persisten retos vinculados a la cultura de cumplimiento en el sector público y privado, especialmente en pequeñas y medianas organizaciones que pueden carecer de infraestructura tecnológica y conocimiento especializado para

implementar programas integrales de protección de datos. A ello se suma la complejidad regulatoria que plantean fenómenos emergentes como la inteligencia artificial, la toma de decisiones automatizadas y las transferencias internacionales de datos, ámbitos en los que la ley puede requerir desarrollo interpretativo constante. Estos elementos evidencian que el desafío actual no radica únicamente en la existencia de un marco normativo avanzado, sino en su aplicación efectiva dentro de un entorno digital dinámico y en permanente transformación.

En este sentido, la Ley Orgánica de Protección de Datos Personales representa la concreción legislativa del proceso de constitucionalización digital, al traducir los principios constitucionales en obligaciones jurídicas específicas y mecanismos de control que garantizan la eficacia material del derecho en entornos digitales.

6. Jurisprudencia constitucional ecuatoriana sobre datos personales

La jurisprudencia reciente de la Corte Constitucional del Ecuador ha desempeñado un papel fundamental en la consolidación del derecho a la protección de datos personales como un derecho fundamental autónomo, especialmente en el contexto de la digitalización y del uso intensivo de tecnologías de tratamiento de información (CCE, 2024; 2025). A través de sus decisiones, el máximo órgano de control constitucional ha definido los alcances del derecho, sus principios rectores y las obligaciones que recaen tanto sobre las instituciones públicas como sobre los actores privados que tratan datos personales. Entre las sentencias más relevantes se encuentran la Sentencia No. 1236-22-EP/24, emitida en 2024, y la Sentencia No. 2172-21-EP/25, adoptada en 2025, las cuales reflejan un avance sustantivo en la comprensión del derecho a la autodeterminación informativa y fortalecen el proceso de constitucionalización digital en el Ecuador.

La Sentencia No. 1236-22-EP/24 constituye un precedente clave en relación con el deber de veracidad, exactitud y actualización de la información contenida en bases de datos institucionales. En este caso, la Corte conoció una acción extraordinaria de protección interpuesta por un ciudadano cuya información personal había sido registrada de manera errónea, lo que afectó su acceso a servicios y generó consecuencias negativas en su vida personal y administrativa. (CCE, 2024). El tribunal determinó que la existencia de datos incorrectos o desactualizados, así como la ausencia de mecanismos eficaces para su corrección, vulnera directamente el derecho a la protección de datos personales.

En su razonamiento, la Corte enfatizó que la administración de bases de datos exige un alto nivel de diligencia y que la responsabilidad de garantizar la calidad de la información recae exclusivamente sobre la entidad que la administra, sin que sea admisible trasladar al titular la carga de probar el error. Asimismo, desarrolló una interpretación amplia del derecho de rectificación como parte esencial del hábeas data, señalando que este no se limita al acceso a la información, sino que permite exigir la corrección inmediata de datos inexactos, incompletos o erróneos. La Corte advirtió que la persistencia de información incorrecta puede generar efectos discriminatorios o afectar el ejercicio de otros derechos fundamentales, por lo que ordenó la corrección de los datos y la adopción de medidas internas para prevenir futuras vulneraciones. (CCE, 2024)

Por su parte, la Sentencia No. 2172-21-EP/25 representó un avance significativo en la interpretación del consentimiento y del principio de finalidad en el tratamiento de datos personales. El caso analizado se relacionó con el uso de información personal por

parte de una entidad pública para fines distintos a aquellos originalmente autorizados por el titular. La Corte sostuvo que el consentimiento debe ser expreso, informado y específico, y que no puede presumirse ni inferirse del simple suministro de datos en un contexto determinado. En consecuencia, cualquier cambio o ampliación de la finalidad del tratamiento exige la obtención de un nuevo consentimiento debidamente informado. La Corte afirmó, además, que el principio de finalidad constituye un límite constitucional al uso de los datos personales, impidiendo que las entidades públicas amplíen unilateralmente los objetivos para los cuales fue recolectada la información. Toda desviación de la finalidad original, incluso cuando persiga fines considerados útiles o convenientes, configura una vulneración constitucional, al convertir los datos en potenciales instrumentos de vigilancia o intervención indebida. (CCE, 2025)

En esta misma sentencia, el tribunal abordó los riesgos asociados a la toma de decisiones automatizadas, estableciendo que los sistemas algorítmicos no pueden sustituir la intervención humana cuando las decisiones afectan derechos fundamentales. Según la Corte, las decisiones basadas exclusivamente en procesos automatizados carecen de legitimidad si no existen mecanismos de supervisión, revisión y garantías suficientes para prevenir errores o discriminaciones derivadas del funcionamiento de los algoritmos. Asimismo, la Corte desarrolló un estándar reforzado sobre el principio de transparencia en el tratamiento de datos personales. Señaló que toda persona tiene derecho a conocer quién administra su información, con qué finalidad se utiliza, qué medidas de seguridad se aplican, durante cuánto tiempo se conservarán los datos y si existe transferencia a terceros. La falta de transparencia, precisó el tribunal, constituye una vulneración autónoma del derecho a la protección de datos, pues impide el ejercicio efectivo de la autodeterminación informativa. (CCE, 2025)

En conjunto, estas decisiones evidencian una línea jurisprudencial orientada a la protección reforzada de los datos personales en el Ecuador. La Corte Constitucional ha consolidado estándares claros en torno a la autodeterminación informativa, la transparencia, el consentimiento informado, la estricta observancia del principio de finalidad y la prohibición de decisiones automatizadas sin supervisión humana significativa. (CCE, 2024; 2025). Este desarrollo jurisprudencial ha permitido que el derecho a la protección de datos evolucione de una garantía meramente formal hacia un mecanismo efectivo de control frente a los riesgos derivados del uso intensivo de datos, consolidándose como un componente esencial del constitucionalismo contemporáneo ecuatoriano.

Desde una perspectiva técnica, resulta necesario precisar que, si bien las sentencias No. 1236-22-EP/24 y No. 2172-21-EP/25 desarrollan estándares robustos en materia de autodeterminación informativa, consentimiento, finalidad y decisiones automatizadas, aún se encuentran en una fase de consolidación progresiva dentro de la jurisprudencia constitucional ecuatoriana. Si bien comparten criterios consistentes y muestran coherencia argumentativa, el número limitado de precedentes en la materia impide afirmar la existencia de una línea jurisprudencial plenamente consolidada en términos de reiteración uniforme y estabilidad prolongada. No obstante, puede advertirse una tendencia clara hacia la construcción de un bloque interpretativo estable en torno a la protección reforzada de los datos personales, lo que permite proyectar una evolución jurisprudencial orientada a fortalecer su carácter autónomo y su eficacia directa en el sistema constitucional ecuatoriano.

La jurisprudencia constitucional confirma que la constitucionalización digital opera como criterio hermenéutico vinculante, permitiendo adaptar el contenido del

derecho a la protección de datos a los desafíos tecnológicos y consolidando su fuerza normativa en el sistema jurídico ecuatoriano.

7. La constitucionalización digital y su influencia en el sistema jurídico ecuatoriano

La constitucionalización digital puede definirse como un fenómeno jurídico evolutivo mediante el cual los principios, valores y derechos reconocidos en la Constitución se proyectan e interpretan en función de los desafíos derivados de la transformación tecnológica. No se trata de la creación de un nuevo orden normativo independiente, sino de un proceso de reinterpretación constitucional que adapta el contenido material de los derechos fundamentales a los entornos digitales donde hoy se desarrollan relaciones sociales, económicas y políticas.

Desde una perspectiva doctrinaria, la constitucionalización digital constituye una manifestación del constitucionalismo contemporáneo caracterizado por la expansión material de los derechos y por la fuerza normativa de la Constitución. Su naturaleza jurídica no radica en ser un derecho autónomo, sino en configurarse como una categoría hermenéutica que orienta la interpretación y aplicación de normas frente a fenómenos tecnológicos como la inteligencia artificial, el tratamiento masivo de datos, la automatización de decisiones y la digitalización de servicios públicos. En este sentido, opera como un criterio estructural que exige que toda innovación tecnológica sea evaluada a la luz de los principios constitucionales de dignidad, proporcionalidad, igualdad y supremacía constitucional.

En el caso ecuatoriano, este proceso adquiere particular relevancia debido al modelo de Estado constitucional de derechos y justicia adoptado en 2008, el cual reconoce la eficacia directa de los derechos fundamentales y habilita su interpretación evolutiva. La constitucionalización digital, por tanto, no representa una ruptura con el texto constitucional, sino una evolución coherente con su estructura garantista, que permite proyectar sus mandatos hacia los escenarios tecnológicos contemporáneos.

Si bien la Constitución de la República del Ecuador de 2008 antecede a la expansión tecnológica de la última década, su estructura incorporó disposiciones que facilitaron el desarrollo posterior de un constitucionalismo digital. (CRE, 2008). El reconocimiento del hábeas data, la protección de datos personales, la inviolabilidad de las comunicaciones y la obligación estatal de garantizar los derechos mediante políticas públicas sentaron las bases para la incorporación progresiva de derechos y garantías digitales, permitiendo al país integrarse tempranamente al debate sobre la protección de la dignidad humana en entornos tecnológicos. Uno de los efectos más relevantes de la constitucionalización digital es la reinterpretación de los derechos fundamentales tradicionales frente a los desafíos tecnológicos actuales. La intimidad se proyecta hacia un ámbito digital protegido frente a prácticas de vigilancia y monitoreo permanente; la honra adquiere nuevas dimensiones ante la existencia de perfiles digitales y la circulación masiva de información en redes; y la igualdad se ve comprometida frente a los riesgos de discriminación derivados del uso de sistemas automatizados. (LOPD, 2021)

En este contexto, la jurisprudencia reciente evidencia una tendencia hacia la protección reforzada de los derechos frente a prácticas como el almacenamiento desproporcionado de información, el tratamiento no transparente de datos y el uso de tecnologías sin controles suficientes. Para ello, la Corte ha incorporado estándares

internacionales, principios tecnológicos contemporáneos y criterios del derecho comparado, consolidando un enfoque garantista acorde con las exigencias del constitucionalismo digital. (CCE, 2024; 2025)

La constitucionalización digital también ha influido directamente en la legislación ecuatoriana; la aprobación de la Ley Orgánica de Protección de Datos Personales en 2021 constituye un ejemplo claro de la materialización normativa del derecho a la autodeterminación informativa reconocido constitucionalmente. Esta ley regula el tratamiento de datos personales e incorpora principios esenciales del constitucionalismo digital, el principio de minimización exige que se recolecte únicamente la información estrictamente necesaria para cumplir una finalidad legítima; el principio de seguridad impone la adopción de medidas técnicas y organizativas destinadas a proteger los datos frente a accesos indebidos o pérdidas; la portabilidad fortalece el control del titular sobre su información al facilitar su transferencia entre servicios; y la transparencia garantiza que las personas conozcan cómo y para qué se utilizan sus datos, asimismo, la creación de la Superintendencia de Protección de Datos Personales responde al mandato constitucional de asegurar la vigencia efectiva de los derechos digitales mediante una autoridad especializada. (LOPDP, 2021)

La constitucionalización digital plantea desafíos específicos en relación con el uso de tecnologías emergentes, entre ellas la inteligencia artificial, cuyo impacto sobre los derechos fundamentales exige un análisis particularizado; la necesidad de establecer límites, garantías y mecanismos de control frente al uso de sistemas automatizados se presenta como una consecuencia directa de la proyección de los principios constitucionales al entorno digital, cuestión que será desarrollada de manera específica en el apartado siguiente.

8. Protección de datos personales frente a la inteligencia artificial

La relación entre la inteligencia artificial y la protección de datos personales ha generado un amplio debate jurídico debido a los riesgos que la automatización, la opacidad algorítmica y la discriminación basada en datos representan para los derechos fundamentales, particularmente la autodeterminación informativa, la privacidad y la igualdad, como advierten (Mejía, 2025); (Arellano, 2025), la inteligencia artificial depende estructuralmente del tratamiento masivo de datos personales para entrenar modelos, identificar patrones y adoptar decisiones automatizadas, lo que incrementa de manera significativa el potencial de afectación a la dignidad humana.

Uno de los principales desafíos se relaciona con la falta de transparencia de los sistemas algorítmicos. Muchos modelos operan como “cajas negras”, lo que impide conocer los criterios de decisión y dificulta la posibilidad de impugnar o revisar decisiones que pueden producir efectos relevantes en los derechos de las personas. (Arellano, 2025). Esta opacidad coloca al titular de los datos en una posición de vulnerabilidad frente a decisiones automatizadas que pueden incidir en el acceso a servicios, beneficios u oportunidades sin control efectivo ni supervisión humana. Otro riesgo central deriva de la recopilación masiva e indiscriminada de datos para el entrenamiento de sistemas de inteligencia artificial. La obtención de información a través de plataformas digitales, redes sociales, sistemas de vigilancia o dispositivos conectados favorece la elaboración de perfiles detallados y la reutilización de datos con finalidades no autorizadas, en contravención del principio de minimización y de la finalidad legítima

del tratamiento, estas prácticas pueden derivar en usos invasivos o discriminatorios de la información personal.

En el ámbito estatal, el uso de tecnologías como el reconocimiento facial, la videovigilancia inteligente o los sistemas predictivos intensifica estos riesgos, pues puede consolidar formas de vigilancia permanente incompatibles con los derechos a la intimidad y a la libertad. Por ello, el tratamiento de datos personales mediante inteligencia artificial debe estar sometido a estrictos criterios de legalidad, necesidad y proporcionalidad, sin que la eficiencia administrativa o la seguridad justifiquen afectaciones desmedidas a los derechos fundamentales.

La Ley Orgánica de Protección de Datos Personales establece obligaciones específicas frente al uso de decisiones automatizadas, entre las que destaca la exigencia de una intervención humana significativa cuando el tratamiento pueda generar efectos jurídicos o impactos relevantes. La ley también reconoce el derecho del titular a ser informado sobre el uso de sistemas automatizados y a solicitar la revisión de las decisiones bajo criterios humanos, reforzando el control sobre su información personal. (LOPDP, 2021)

Un elemento especialmente relevante es la existencia de sesgos algorítmicos. Los sistemas de inteligencia artificial reproducen los sesgos presentes en los datos con los que son entrenados, lo que puede traducirse en prácticas discriminatorias que afectan de manera desproporcionada a grupos históricamente vulnerables. (Arellano, et al., 2025). En contextos como el ecuatoriano, estas dinámicas representan una amenaza directa al principio constitucional de igualdad y no discriminación.

Frente a estos riesgos, la transparencia algorítmica y las evaluaciones de impacto en protección de datos se consolidan como mecanismos esenciales de control. La obligación de informar sobre el funcionamiento general de los sistemas automatizados y de identificar anticipadamente los riesgos del tratamiento resulta indispensable para garantizar el ejercicio efectivo de los derechos y prevenir vulneraciones graves. En conjunto, la protección de datos personales frente a la inteligencia artificial constituye uno de los desafíos más complejos del constitucionalismo digital, que exige un equilibrio entre innovación tecnológica y salvaguarda efectiva de los derechos fundamentales desde una perspectiva ética y garantista. (LOPDP, 2021).

9. Responsabilidad del Estado en el tratamiento de datos personales

La responsabilidad del Estado en el tratamiento de datos personales adquiere un carácter reforzado dentro del sistema jurídico ecuatoriano, en atención a su posición de garante de los derechos fundamentales y al volumen de información sensible que administra. (LOPDP, 2021). Las instituciones públicas gestionan datos biométricos, de salud, financieros, judiciales y administrativos, cuya vulneración puede generar afectaciones graves a la dignidad, la seguridad jurídica y la vida privada de las personas. La Constitución de la República del Ecuador reconoce la protección de datos personales como un derecho fundamental, lo que obliga al Estado a adoptar medidas efectivas para garantizar la licitud, confidencialidad, proporcionalidad y seguridad del tratamiento de información personal. (CRE, 2008). Este deber no se agota en el cumplimiento formal de la normativa, sino que exige una actuación estructural y permanente que abarque todas las fases del ciclo de vida de los datos, desde su recolección hasta su eliminación.

La responsabilidad estatal se justifica, en primer lugar, por la naturaleza altamente sensible de los datos que concentra el sector público, cuya filtración puede ocasionar daños irreversibles. En segundo lugar, porque existe una relación de supremacía institucional que obliga a las personas a proporcionar información para acceder a servicios, cumplir obligaciones legales o realizar trámites administrativos, lo que limita la libertad del consentimiento y exige mayores garantías por parte del Estado. Finalmente, las decisiones públicas basadas en datos personales pueden incidir directamente en el acceso a derechos, beneficios o servicios, por lo que cualquier irregularidad en su manejo puede afectar la igualdad, el debido proceso o la honra por lo cual la Constitución y la Ley Orgánica de Protección de Datos Personales imponen obligaciones claras a la administración pública; la recopilación de datos debe responder a una finalidad legítima, expresa y estrictamente necesaria, sin que la eficiencia administrativa justifique prácticas de acumulación masiva de información. (CRE, 2008; LOPDP, 2021).

Desde una perspectiva jurídica, la responsabilidad del Estado en el tratamiento indebido de datos personales puede manifestarse en tres dimensiones complementarias: administrativa, civil y constitucional. En el ámbito administrativo, las entidades públicas y sus funcionarios pueden ser objeto de procedimientos sancionatorios cuando incumplen las obligaciones previstas en la Ley Orgánica de Protección de Datos Personales, particularmente en lo relativo a seguridad, finalidad, consentimiento y minimización. Esta responsabilidad puede derivar en sanciones disciplinarias, multas institucionales o medidas correctivas impuestas por la autoridad de control competente.

En el plano civil, la vulneración del derecho a la protección de datos puede generar la obligación de reparar los daños materiales e inmateriales ocasionados al titular de la información, conforme al régimen general de responsabilidad extracontractual del Estado. La filtración, uso indebido o tratamiento ilícito de datos puede producir afectaciones patrimoniales, daño moral, afectación a la honra o perjuicios derivados de decisiones administrativas erróneas basadas en información incorrecta.

En el ámbito constitucional, la responsabilidad estatal se activa cuando el tratamiento indebido configura una vulneración directa de derechos fundamentales, lo que habilita la interposición de garantías jurisdiccionales como el hábeas data o la acción extraordinaria de protección. En estos casos, la respuesta jurídica no se limita a la cesación de la conducta lesiva, sino que debe incorporar el principio de reparación integral, que comprende medidas de restitución, indemnización, rehabilitación, garantías de no repetición y, cuando corresponda, satisfacción.

La articulación de estos tres niveles de responsabilidad evidencia que la protección de datos personales no se reduce a una obligación programática, sino que integra un sistema estructurado de consecuencias jurídicas frente a su vulneración, reforzando el carácter garantista del Estado constitucional de derechos.

La extensión de obligaciones tanto al sector público como al privado demuestra que la constitucionalización digital no se limita a un fenómeno interpretativo, sino que transforma estructuralmente el modelo de responsabilidad en materia de tratamiento de datos personales.

Conclusiones

El problema jurídico planteado en este artículo consistió en determinar si el marco constitucional y legal ecuatoriano permite considerar la protección de datos personales

como un derecho fundamental autónomo dentro del modelo de Estado constitucional de derechos y justicia, y si dicho reconocimiento es suficiente para enfrentar los desafíos derivados de la digitalización y del uso intensivo de tecnologías emergentes. El análisis desarrollado demuestra que el ordenamiento jurídico ecuatoriano ha avanzado de manera significativa en la consolidación de este derecho, tanto a nivel normativo como jurisprudencial, configurando un proceso progresivo de constitucionalización digital.

El objetivo del estudio, orientado a examinar el sustento constitucional, legal y jurisprudencial de la protección de datos personales en el Ecuador, se cumple al evidenciar que existe una estructura normativa coherente que articula principios, garantías jurisdiccionales y mecanismos institucionales de control. Sin embargo, también se constata que la eficacia real del sistema depende de su aplicación práctica, de la consolidación jurisprudencial y del fortalecimiento institucional de los órganos encargados de su supervisión.

El establecimiento de la Superintendencia de Protección de Datos Personales complementa este sistema normativo, permitiendo la supervisión efectiva, la imposición de sanciones y la creación de políticas públicas orientadas a fortalecer la cultura de protección de datos en la ciudadanía. El análisis revela que los desafíos vinculados a la digitalización no se limitan a la mera administración técnica de datos, sino que involucran consideraciones éticas, políticas y sociales que inciden directamente en la estructura misma del Estado constitucional de derechos.

La constitucionalización digital demuestra que los derechos tradicionales (como la intimidad, la honra, la igualdad y el debido proceso) adquieren nuevas dimensiones en entornos mediatizados por algoritmos, inteligencia artificial y plataformas digitales. Este fenómeno exige reinterpretaciones constantes, así como la adopción de enfoques preventivos que anticipen los riesgos y garanticen la vigencia efectiva de los derechos. En este sentido, la Corte Constitucional ha desempeñado un rol fundamental al desarrollar estándares jurisprudenciales que fortalecen el derecho a la autodeterminación informativa y establecen límites claros al uso excesivo, desproporcionado o no transparente de datos personales.

La inteligencia artificial constituye uno de los mayores desafíos del constitucionalismo digital ecuatoriano. Su capacidad para procesar grandes volúmenes de datos, generar perfiles, tomar decisiones automatizadas y operar de manera opaca plantea riesgos significativos que pueden afectar derechos fundamentales como la igualdad, la privacidad y la autonomía personal. El país se enfrenta al reto de asegurar que el uso de estas tecnologías se desarrolle dentro de límites éticos y jurídicos claramente definidos, con supervisión humana efectiva, transparencia suficiente y mecanismos adecuados para prevenir sesgos, discriminación, vigilancia indebida y afectaciones desproporcionadas.

La LOPDP ofrece herramientas importantes para enfrentar estos desafíos, pero su eficacia dependerá de la capacidad institucional para hacer cumplir sus disposiciones y adaptarlas a los avances tecnológicos constantes. El estudio también evidencia que el Estado ecuatoriano tiene una responsabilidad reforzada en materia de tratamiento de datos personales. Esto se debe no solo a la cantidad de información que administra, sino también a la posición de supremacía institucional que le permite exigir datos a la ciudadanía sin que el consentimiento pueda considerarse plenamente libre.

En este sentido, la protección de datos personales no puede entenderse únicamente como una regulación técnica del flujo de información, sino como una manifestación estructural del constitucionalismo contemporáneo, que redefine las relaciones entre

individuo, Estado y tecnología. La tesis central del artículo queda confirmada: la constitucionalización digital en el Ecuador no constituye una categoría retórica, sino un proceso jurídico real que transforma el alcance de los derechos fundamentales y exige una interpretación dinámica capaz de responder a los riesgos de la inteligencia artificial, la automatización y la economía de datos. El desafío pendiente radica en consolidar estos avances mediante una aplicación rigurosa, una línea jurisprudencial estable y una cultura institucional orientada a la protección efectiva de la dignidad humana en entornos digitales.

Recomendaciones

A partir de los hallazgos del presente estudio, se recomienda profundizar el desarrollo doctrinario y jurisprudencial del derecho a la protección de datos personales como derecho fundamental autónomo, consolidando una línea interpretativa estable que delimite con claridad su diferencia conceptual y funcional frente a la privacidad y la intimidad. Esta precisión resulta indispensable para evitar confusiones hermenéuticas y garantizar una tutela más efectiva en entornos digitales complejos.

En el plano institucional, se recomienda fortalecer la capacidad técnica y operativa de la Superintendencia de Protección de Datos Personales, asegurando su autonomía, recursos suficientes y mecanismos eficaces de fiscalización, especialmente frente a entidades públicas y grandes actores tecnológicos. La eficacia del sistema dependerá no solo de la existencia de la norma, sino de su aplicación rigurosa y sostenida.

En materia jurisdiccional, resulta pertinente promover la consolidación de una línea jurisprudencial uniforme en torno al consentimiento informado, el principio de finalidad, la transparencia algorítmica y la prohibición de decisiones automatizadas sin supervisión humana significativa. La estabilidad de estos estándares permitirá dotar de mayor seguridad jurídica al sistema y reforzar la protección frente a prácticas invasivas o discriminatorias.

Finalmente, frente al avance de la inteligencia artificial y los sistemas de tratamiento masivo de datos, se recomienda incorporar de manera sistemática evaluaciones de impacto en derechos fundamentales, así como mecanismos de auditoría y supervisión preventiva que permitan anticipar riesgos estructurales. La innovación tecnológica debe integrarse dentro de un marco de responsabilidad reforzada, especialmente cuando interviene el Estado, cuyo deber de garante exige niveles superiores de diligencia, transparencia y rendición de cuentas.

Bibliografía:

1. Arellano-Sarasti, P., Colón-Ferruzola, E., & Galarza-Castro, C. X. (2025). Hacia una inteligencia artificial jurídicamente confiable: análisis crítico de su regulación en Ecuador. *MQR Investigar*, 9(2). <https://doi.org/10.56048/MQR20225.9.2.2025.e737>
2. Asamblea Nacional del Ecuador. (26 de mayo de 2021). Ley Orgánica de Protección de Datos Personales (Registro Oficial Supl. 459).

<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf> .

3. Asamblea Nacional del Ecuador. (26 de mayo de 2021). Ley Orgánica de Protección de Datos Personales (texto oficial — copia). <https://procuraduria.utpl.edu.ec/sitios/documentos/NormativasPublicas/Ley%20de%20O rg%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos.pdf> .
4. Autor/es anónimo(s). (2024). Alcance del hábeas data: protección jurídica en la era digital en Ecuador. ResearchGate (prepublicación). Recuperado de https://www.researchgate.net/publication/388295965_Alcance_del_Habeas_Data_Proteccion_Juridica_en_la_Era_Digital_en_Ecuador.
5. Ávila Merino, C. E. (2019). El derecho a la intimidad y la protección de datos personales en el marco jurídico ecuatoriano [Trabajo de titulación, Universidad Central del Ecuador]. Repositorio UCE. <https://www.dspace.uce.edu.ec/entities/publication/d31b7f95-9183-4185-b8a4-a3ebe72370b7/full>
6. Ávila Merino, C. E. (2019). El derecho a la intimidad y la protección de datos personales en el marco jurídico ecuatoriano [Trabajo de titulación]. Universidad Central del Ecuador. <https://www.dspace.uce.edu.ec/entities/publication/d31b7f95-9183-4185-b8a4-a3ebe72370b7/full>.
7. Constitución de la República del Ecuador. (2008). Constitución de la República del Ecuador (versión consolidada). https://defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf.
8. Corte Constitucional del Ecuador. (2 de mayo de 2024). Sentencia No. 151-21-JD-24 (resolución sobre hábeas data y protección de datos personales). <https://www.cortenacional.gob.ec/cnj/images/pdf/CC/Sentencia-151-21-JD-24.pdf> .
9. Corte Constitucional del Ecuador. (28 de noviembre de 2024). Sentencia No. 1236-22- EP/24 (decisión relacionada con tutela y hábeas data). https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJYXJwZXRhIjoIdHJhbWl0ZSI6InV1aWQiOiJiYWJiNGFmYS04MzVjLTQzODktYmlzOS03ZGRiYzI2ZmZlMzAucGRmIn0%3D.
10. Corte Constitucional del Ecuador. (5 de junio de 2025). Sentencia No. 2172-21-EP/25 (revisión sobre procedencia y alcance del hábeas data). https://www.fielweb.com/App_Themes/InformacionInteres/b761ee0f-bf70-4a09-92e8-4becd8f4b278.pdf.
11. Dirección Nacional de Registros Públicos. (s. f.). Base legal – Ejercicio de los derechos de protección de datos personales. <https://www.registrospublicos.gob.ec/base-legal-ejercicio-de-los-derechos-de-proteccion-de-datos-personales/>
12. Dirección Nacional de Registros Públicos. (s. f.). La protección de datos personales es un derecho fundamental reconocido en la Constitución del Ecuador. <https://www.registrospublicos.gob.ec/la-proteccion-datos-personales-es-un-derecho-fundamental-reconocido-en-la-constitucion-del-ecuador/>
13. Hernández-Sotomayor, G., & Moscoso-Parra, R. K., Álvarez-Carrión, J. A. (2025). Protección de datos personales y derechos humanos en Ecuador: Desafíos en la

era de la inteligencia artificial y la digitalización. MQR Investigar, 25(9.2), e489. <https://doi.org/10.56048/MQR20225.9.2.2025.e489>

14. Hidalgo, G. F. A. (2023). Análisis de la protección de datos personales en las redes y su relación con el marco constitucional ecuatoriano. Dilemas Contemporáneos. <https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/download/3487/3444/>.

15. Kosinski, M., & Forrest, A. (n.d.). ¿Qué es la protección de los datos? IBM Think. <https://www.ibm.com/es-es/think/topics/data-privacy>

16. Mejía Terán, D. F. (2025). Caso 700 IA: entre la protección de datos personales y el uso de la inteligencia artificial. URU: Revista de Comunicación y Cultura, 11, 101-116. Universidad Andina Simón Bolívar, Sede Ecuador. <https://repositorio.uasb.edu.ec/handle/10644/10358>

17. Muñoa, T., Villacís Chávez, S. S., & Villacís Londoño, H. S. (2022). Dimensiones jurídicas sobre la protección de los datos personales en los medios tecnológicos. ReHuSo: Revista de Ciencias Humanísticas y Sociales, 10(2). <https://doi.org/10.33936/rehuso.v10i2.6922>. <https://revistas.utm.edu.ec/index.php/Rehuso/article/view/6922>.

18. Ordóñez Pineda, L. (2021). El derecho fundamental a la protección de datos personales en Ecuador. Perspectivas, (5). <https://revistas.ucalp.edu.ar/index.php/Perspectivas/article/view/193>

19. Pérez, A. (2024). Desafíos del hábeas data en la protección de datos personales en Ecuador. Epsir — Revista (artículo/monografía). <https://epsir.net/index.php/epsir/article/download/1842/1090/7922>.

20. Piñar Mañas, J.L (2016). El derecho fundamental y de protección de datos personales Madrid: Agencia Español de Protección de Datos. <https://www.aepd.es/es/documento/el-derecho-fundamental-a-la-proteccion-de-datos-personales.pdf>

21. Presidencia / Secretaría técnica (Reglamento). (2023). Decreto Ejecutivo / Reglamento relacionado con la Ley Orgánica de Protección de Datos Personales. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo- No.-904.pdf>.

22. PwC Ecuador. (n.d.). Todo lo que debes conocer sobre la Protección de Datos Personales. PwC. <https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html>

23. Real Academia Española. (2025). Protección de datos. En Diccionario panhispánico del español jurídico. <https://dpej.rae.es/lema/protecci%C3%B3n-de-datos>

24. Registro de la Propiedad (Registro Público). (s. f.). La protección de datos personales es un derecho fundamental reconocido en la Constitución del Ecuador. <https://www.registropublicos.gob.ec/la-proteccion-datos-personales-es-un-derecho-fundamental-reconocido-en-la-constitucion-del-ecuador/>.

25. Rodotá, S. (2009). La vida en la sociedad de la vigilancia. Madrid: Editorial Trotta. <https://www.trotta.es>

26. SPDP (Ecuador). (s. f.). Política para el tratamiento de datos personales en la Corte Constitucional del Ecuador. <https://www.corteconstitucional.gob.ec/265720-2/>