

Derechos constitucionales y protección de datos privados de los ecuatorianos

Constitutional rights and protection of private data of ecuadorians

Mateo Nicolás Mora Abril

Universidad Tecnológica Indoamérica. Ecuador.

mmora20@indoamerica.edu.ec

<https://orcid.org/0009-0009-8517-8505>

Estefanía Cristina Mayorga Mayorga

Universidad Tecnológica Indoamérica. Ecuador.

emayorga5@indoamerica.edu.ec

<https://orcid.org/0009-0000-1495-2633>

Fecha de recepción: 19 de marzo de 2026

Fecha de aceptación: 07 de junio de 2026

Fecha de publicación: 15 de julio de 2026

Como citar: Mora Abril, M. N. y Mayorga Mayorga, E. C. (2026). Derechos constitucionales y protección de datos privados de los ecuatorianos. *KIRIA: Revista Científica Multidisciplinaria*. Ed. Esp. 1(3), pp. 117-132. <https://doi.org/10.53877/nf7a8h27>

RESUMEN

La protección de los datos personales constituye un derecho fundamental que garantiza la privacidad, la dignidad y el control de las personas sobre su información en la era digital. El avance tecnológico y el tratamiento masivo de datos han incrementado los riesgos de vulneración de estos derechos, lo que exige mecanismos jurídicos eficaces para su protección. El objetivo de este artículo es analizar la eficacia de los mecanismos jurídicos y constitucionales vigentes en Ecuador frente a las dinámicas de vigilancia, inferencia y control derivadas del tratamiento masivo de datos personales. La investigación adopta un enfoque cualitativo, sustentado en el análisis doctrinal, normativo y jurisprudencial, con un alcance analítico que examina la relación entre el desarrollo tecnológico, las vulneraciones digitales y la respuesta del ordenamiento jurídico ecuatoriano. Los resultados evidencian que, pese a la existencia de un marco normativo de protección, persisten desafíos para enfrentar las nuevas formas de tratamiento y las filtraciones de datos. Se concluye que la protección de los datos personales es un derecho autónomo indispensable para garantizar la privacidad, la seguridad, la autodeterminación informativa y la confianza en las instituciones responsables del tratamiento de información.

PALABRAS CLAVE: derechos, dignidad, información, privacidad y protección.

ABSTRACT

The protection of personal data constitutes a fundamental right that guarantees individuals' privacy, dignity, and control over their personal information in the digital age. Technological advances and the large-scale processing of personal data have increased the risks of violations of these rights, making effective legal mechanisms essential for their protection. This article aims to analyze the effectiveness of the legal and constitutional mechanisms currently in force

in Ecuador in addressing the challenges posed by surveillance, inference, and control resulting from the large-scale processing of personal data. The research adopts a qualitative approach based on doctrinal, legal, and jurisprudential analysis, with an analytical scope that examines the relationship between technological development, digital rights violations, and the response of the Ecuadorian legal system. The findings indicate that, despite the existence of a legal framework for data protection, significant challenges remain in addressing emerging forms of data processing and data breaches. It is concluded that personal data protection is an autonomous fundamental right essential to safeguarding privacy, security, informational self-determination, and public trust in institutions responsible for processing personal information.

KEYWORDS: rights, dignity, information, privacy and protection.

INTRODUCCIÓN

La transformación digital ha modificado significativamente la forma en que las personas interactúan, se comunican y desarrollan sus actividades cotidianas. El uso masivo de internet, redes sociales, aplicaciones móviles, sistemas automatizados e inteligencia artificial ha facilitado el acceso a servicios y la circulación de información; sin embargo, también ha incrementado los riesgos relacionados con el tratamiento, almacenamiento y difusión de datos personales, generando nuevos desafíos para la protección de los derechos fundamentales.

Actualmente, los datos personales constituyen un recurso de gran valor para instituciones públicas, empresas privadas y plataformas digitales, debido a que permiten analizar comportamientos, preferencias y características de los usuarios. Esta situación ha fortalecido la preocupación por la privacidad, la intimidad y la autodeterminación informativa frente a prácticas como la vigilancia digital, el perfilamiento y el uso masivo de bases de datos.

En Ecuador, la protección de datos personales cuenta con reconocimiento constitucional. La Constitución de la República del Ecuador (2008), en su artículo 66 numeral 19, garantiza el derecho a la protección de datos de carácter personal, otorgando a las personas la facultad de acceder, conocer, decidir y controlar la información que les concierne. Además, establece que su tratamiento requiere autorización del titular o fundamento legal.

Posteriormente, la Ley Orgánica de Protección de Datos Personales fortaleció este marco mediante principios, obligaciones y mecanismos orientados a garantizar el adecuado tratamiento de la información. No obstante, la existencia de normas no asegura por sí misma una protección efectiva, pues persisten desafíos relacionados con filtraciones de datos, uso indebido de información y limitaciones en la aplicación práctica de estas garantías jurídicas.

En este contexto, Vaca (2026) sostiene que,

Pese al reconocimiento constitucional del derecho a la protección de datos personales en Ecuador, persisten dificultades relacionadas con su aplicación efectiva y con su comprensión como un derecho autónomo. Según el autor, la vulneración de datos personales continúa siendo frecuente en ámbitos como la administración pública, el sistema financiero y los entornos digitales, situación que genera escenarios de inseguridad jurídica y limita la tutela efectiva de los ciudadanos. (p.3)

Ante esta realidad, resulta necesario analizar la capacidad de respuesta del ordenamiento jurídico ecuatoriano frente a los desafíos derivados del tratamiento masivo de datos personales. El desarrollo de tecnologías capaces de recopilar, procesar y almacenar grandes volúmenes de información requiere mecanismos de protección eficaces que garanticen la privacidad, la intimidad, la libertad y la dignidad de las personas.

En este contexto, la investigación plantea la siguiente pregunta: ¿En qué medida los mecanismos jurídicos y constitucionales vigentes en Ecuador garantizan la protección efectiva de los derechos fundamentales frente a las dinámicas de vigilancia, inferencia y control derivadas del tratamiento masivo de datos personales en entornos digitales?

El objetivo es analizar la eficacia de dichos mecanismos en la protección de los derechos fundamentales. La investigación adquiere relevancia porque la protección de datos personales constituye una garantía constitucional vinculada con la privacidad, la autodeterminación informativa y la seguridad jurídica, más allá de una simple dimensión tecnológica. Por ello, es necesario examinar las herramientas jurídicas existentes y los desafíos que enfrenta su aplicación ante la evolución tecnológica y el uso creciente de información personal.

MATERIALES Y MÉTODOS

La presente investigación adopta un enfoque cualitativo, orientado al análisis doctrinal, normativo y jurisprudencial de la protección de datos personales en Ecuador. Este enfoque permite comprender cómo el ordenamiento jurídico ecuatoriano enfrenta los desafíos derivados del tratamiento masivo de información personal en entornos digitales y la eficacia de los mecanismos destinados a garantizar los derechos fundamentales.

El estudio posee un alcance descriptivo y analítico. Es descriptivo porque examina los conceptos, principios y normas que regulan la protección de datos personales, así como las garantías constitucionales existentes. Es analítico porque aborda críticamente la relación entre el desarrollo tecnológico, las vulneraciones digitales y la respuesta jurídica del Estado ecuatoriano.

Se emplea el método analítico-jurídico mediante el estudio de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, doctrina especializada y jurisprudencia nacional e internacional relacionada con la autodeterminación informativa. Asimismo, se utiliza la revisión documental y bibliográfica como técnica de investigación, mediante el análisis de artículos científicos, normativa vigente, sentencias y documentos especializados. Estas fuentes permiten fundamentar el marco teórico y jurídico necesario para comprender los retos actuales de la protección de datos personales.

En consecuencia, la metodología seleccionada posibilita examinar de manera integral la protección de datos personales como una garantía constitucional, permitiendo determinar la eficacia de los mecanismos jurídicos existentes frente a las nuevas dinámicas de vigilancia, control e inferencia derivadas del tratamiento masivo de información en la era digital.

Derechos Fundamentales y Protección de Datos Personales

La protección de datos personales constituye una de las expresiones más relevantes de los derechos fundamentales en la sociedad digital contemporánea. El desarrollo tecnológico ha transformado la forma en que las personas generan, comparten y almacenan información, permitiendo que grandes volúmenes de datos sean recopilados y procesados por instituciones públicas, empresas privadas y plataformas digitales. Esta realidad ha incrementado los riesgos para la privacidad y ha evidenciado la necesidad de fortalecer mecanismos jurídicos que garanticen el control sobre la información personal.

Los derechos fundamentales son garantías inherentes a la persona humana destinadas a proteger su dignidad, libertad e igualdad, estableciendo límites al poder estatal y a las actuaciones privadas que puedan afectar la esfera individual. En el entorno digital, la protección de datos personales se ha consolidado como un derecho esencial para preservar la autonomía y el control de las personas sobre su información.

Este reconocimiento responde a los nuevos riesgos derivados de tecnologías capaces de recopilar, procesar y analizar datos mediante sistemas automatizados. A diferencia de las amenazas tradicionales a la privacidad, actualmente la información personal puede ser utilizada para generar perfiles detallados, por lo que su protección adquiere una dimensión constitucional que supera la concepción clásica de la intimidad.

Concepto de derechos fundamentales

Los derechos fundamentales constituyen garantías jurídicas esenciales reconocidas a toda persona por su condición humana. Su finalidad consiste en proteger valores indispensables para el desarrollo integral del individuo, tales como la dignidad, la libertad, la igualdad, la intimidad y la seguridad jurídica. Estos derechos no son concesiones del Estado, sino prerrogativas inherentes a la persona que deben ser respetadas, protegidas y garantizadas por los poderes públicos.

En este sentido, Mata (2015) sostiene que,

La dignidad humana constituye el fundamento ético de los derechos humanos, aunque para alcanzar una protección efectiva resulta necesario incorporarlos al derecho positivo mediante mecanismos jurídicos que permitan su realización práctica. Según el autor, la protección de la dignidad representa una construcción permanente que debe adaptarse a las necesidades y desafíos de cada contexto histórico. (p. 48)

La postura doctrinal expuesta permite comprender que los derechos fundamentales no permanecen estáticos, sino que evolucionan conforme cambian las condiciones sociales, económicas y tecnológicas. En consecuencia, la protección de datos personales surge como una respuesta jurídica frente a los nuevos escenarios de vulneración que caracterizan a la sociedad digital, donde la información se ha convertido en un elemento esencial para el ejercicio de múltiples derechos.

Evolución de los derechos frente al desarrollo tecnológico

La evolución tecnológica ha generado profundas transformaciones en la forma de comprender y proteger los derechos fundamentales. El avance de internet, las redes sociales, la inteligencia artificial, los sistemas biométricos y las plataformas digitales ha ampliado significativamente la capacidad de recopilar y procesar información sobre las personas, creando desafíos que no existían en etapas anteriores.

Loja (2020) señala que,

El desarrollo de sistemas informáticos ha incrementado la importancia de la privacidad y la protección de datos personales, debido a que el tratamiento de información mediante herramientas tecnológicas puede comprometer derechos fundamentales cuando no existen mecanismos adecuados de control y supervisión. Asimismo, destaca que la privacidad ya no constituye únicamente una cuestión individual, sino una responsabilidad colectiva que exige la adopción de medidas destinadas a prevenir usos indebidos de la información. (pp. 567-570)

Este criterio evidencia que los derechos fundamentales deben interpretarse de manera dinámica para responder a las nuevas formas de vulneración derivadas de la tecnología. En la actualidad, la afectación a la privacidad puede producirse mediante el tratamiento masivo de datos, el monitoreo digital, la utilización de algoritmos predictivos o la implementación de sistemas de reconocimiento biométrico, circunstancias que exigen una protección jurídica especializada.

Derecho a la privacidad e intimidad

La privacidad y la intimidad constituyen derechos fundamentales estrechamente vinculados con la protección de datos personales. Ambos buscan garantizar que las personas puedan desarrollar aspectos esenciales de su vida sin injerencias arbitrarias o no autorizadas por parte del Estado o de particulares.

La privacidad protege el ámbito personal de cada individuo frente a intromisiones indebidas, comprendiendo aspectos relacionados con las comunicaciones, la imagen, la vida familiar y las decisiones individuales. Por su parte, la intimidad se refiere a aquellas dimensiones más reservadas de la existencia humana, tales como la información médica, las creencias personales, las relaciones afectivas o cualquier otro aspecto que la persona desee mantener fuera del conocimiento público

Al respecto, Pfeffer (2015) afirma que,

Los derechos a la intimidad, privacidad, honor e imagen constituyen bienes jurídicos fundamentales que emanan de la propia personalidad humana. Según el autor, estos derechos permiten garantizar el libre desarrollo de la persona y protegerla frente a intromisiones externas que afecten su esfera privada. (p. 465).

Desde esta perspectiva, la protección de datos personales se configura como una herramienta indispensable para garantizar la efectividad de estos derechos en entornos digitales. La recopilación y tratamiento de información sin consentimiento, así como la difusión no autorizada de datos personales, pueden afectar directamente la privacidad y la intimidad de los ciudadanos, generando consecuencias jurídicas y personales de considerable relevancia.

Autodeterminación informativa

La autodeterminación informativa constituye uno de los pilares fundamentales de la protección de datos personales. Este concepto reconoce la facultad de toda persona para decidir sobre el tratamiento de la información que le concierne, permitiéndole conocer, controlar y determinar la forma en que sus datos son utilizados por terceros.

Sobre este punto, De la Cueva (2008) sostiene que,

La protección de datos personales constituye un derecho fundamental autónomo cuyo objetivo consiste en proporcionar a los individuos mecanismos efectivos para controlar el uso de la información relacionada con su persona. Esta concepción supera la visión tradicional de la intimidad y reconoce que el titular debe mantener capacidad de decisión sobre el destino de sus datos personales. (pp. 18, 35 y 38).

La relevancia de este planteamiento resulta evidente en el contexto actual, donde la información personal es constantemente recopilada por entidades públicas y privadas. La autodeterminación informativa permite equilibrar la relación existente entre el titular de los datos y quienes los administran, garantizando que el tratamiento de la información se realice conforme a principios de legalidad, transparencia y respeto a los derechos fundamentales.

Concepto de datos personales

Los datos personales comprenden toda información que identifica o permite identificar directa o indirectamente a una persona natural. Esta información puede manifestarse a través de múltiples formatos y soportes, incluyendo registros físicos, documentos digitales, imágenes, audios, bases de datos o cualquier otro medio que permita individualizar a una persona.

Dentro de esta categoría se encuentran datos como nombres, números de identificación, direcciones domiciliarias, correos electrónicos, números telefónicos,

fotografías, ubicaciones geográficas, historiales médicos, datos financieros y registros digitales generados por el uso cotidiano de tecnologías de información y comunicación.

La importancia jurídica de los datos personales radica en que constituyen una extensión de la identidad del individuo. Por esta razón, su tratamiento debe realizarse respetando los principios y garantías establecidos por el ordenamiento jurídico, evitando prácticas que puedan comprometer la privacidad, la dignidad o la libertad de las personas.

Diferencia entre datos personales, sensibles y biométricos

La clasificación de los datos personales permite establecer el nivel de protección jurídica requerido para cada tipo de información. En general, los datos personales comprenden toda información que permite identificar a una persona; sin embargo, ciertas categorías requieren una tutela reforzada por los riesgos asociados a su tratamiento.

Los datos sensibles revelan aspectos íntimos de la persona, como origen étnico, creencias religiosas, ideología, orientación sexual, estado de salud o información genética. Su uso indebido puede ocasionar discriminación, exclusión y vulneraciones a derechos fundamentales.

Dentro de esta categoría se encuentran los datos biométricos, que permiten identificar a una persona mediante características físicas, fisiológicas o conductuales únicas, como huellas dactilares, reconocimiento facial, iris o voz. Su importancia jurídica radica en que, debido a su carácter permanente, una vulneración puede generar consecuencias difíciles de revertir, aumentando los riesgos derivados de su tratamiento inadecuado.

Cuadro 1

Diferencias entre datos personales, datos sensibles y datos biométricos

Categoría	Definición	Ejemplos	Nivel de protección
Datos personales	Información que identifica o permite identificar directa o indirectamente a una persona natural.	Nombre, número de cédula, correo electrónico, dirección domiciliaria, número telefónico, fotografía, firma, usuario de redes sociales.	Deben ser tratados conforme a los principios de legalidad, finalidad, proporcionalidad y seguridad establecidos en la normativa vigente.
Datos sensibles	Información que revela aspectos relacionados con la esfera más íntima de la persona y cuyo tratamiento indebido puede generar discriminación o afectar derechos fundamentales.	Estado de salud, origen étnico, convicciones religiosas, ideología, orientación sexual, datos genéticos y discapacidad.	Requieren medidas reforzadas de protección debido al riesgo que implica su utilización indebida.
Datos biométricos	Categoría especial de datos sensibles que permiten identificar a una persona mediante características físicas, fisiológicas o conductuales únicas.	Huella dactilar, reconocimiento facial, iris, retina, voz, geometría de la mano y patrones biométricos.	Su protección exige estándares más rigurosos debido a que no pueden modificarse fácilmente una vez comprometidos.

Fuente: Constitución de la República del Ecuador (2008) y Ley Orgánica de Protección de Datos Personales (2021). Elaboración propia.

Roldán (2021) sostiene que,

La protección de datos personales y la autodeterminación informativa requieren mecanismos jurídicos específicos que permitan garantizar el control efectivo de la información por parte de su titular. Esta perspectiva resulta particularmente importante respecto de los datos biométricos, debido a que su utilización implica niveles superiores de riesgo para la privacidad y la seguridad individual. (pf.1)

La diferenciación entre datos personales, sensibles y biométricos constituye una herramienta jurídica que permite establecer el nivel de protección requerido para cada tipo de información. Mientras mayor sea el riesgo que implica su tratamiento para los derechos fundamentales, mayores deben ser las obligaciones de quienes administran dichos datos.

En este sentido, los datos personales forman parte de la protección de derechos como la identidad, privacidad, intimidad y libertad individual. Aunque su tratamiento contribuye al desarrollo tecnológico y a la prestación de servicios, el uso sin consentimiento, transparencia o medidas adecuadas de seguridad puede generar graves vulneraciones. Por ello, la protección de datos personales representa una garantía constitucional esencial para preservar la dignidad humana y asegurar el ejercicio efectivo de las libertades en los entornos digitales.

Filtraciones de Datos Personales y Responsabilidad Jurídica de Instituciones Públicas y Privadas en Ecuador

Las filtraciones de datos personales constituyen una de las principales amenazas para los derechos fundamentales en la sociedad digital contemporánea. El uso creciente de plataformas tecnológicas, servicios digitales e instituciones públicas y privadas ha incrementado la recopilación y procesamiento de información personal, generando beneficios, pero también nuevos riesgos para la seguridad de los datos.

La exposición indebida de información trasciende el ámbito tecnológico, pues puede afectar derechos como la privacidad, la intimidad, la honra, la autodeterminación informativa y la dignidad humana. Por ello, las filtraciones deben comprenderse como vulneraciones jurídicas que requieren medidas de prevención, control y reparación.

En Ecuador, la digitalización ha aumentado el tratamiento de datos relacionados con identidad, salud, educación, finanzas e información biométrica, cuya gestión debe ajustarse a la Constitución y a la Ley Orgánica de Protección de Datos Personales. Sus consecuencias pueden incluir suplantación de identidad, fraude, discriminación y exposición de información sensible, evidenciando la necesidad de fortalecer los mecanismos jurídicos e institucionales de protección.

Fundamentos teóricos de las filtraciones de datos personales

Las filtraciones de datos personales pueden definirse como incidentes de seguridad que comprometen la confidencialidad, integridad o disponibilidad de información relacionada con personas naturales. Estas situaciones se producen cuando datos personales son accedidos, divulgados, alterados, destruidos o utilizados por sujetos no autorizados, generando riesgos para los derechos e intereses legítimos de sus titulares.

La gravedad de una filtración depende de diversos factores, entre ellos la naturaleza de la información comprometida, la cantidad de personas afectadas, el nivel de protección existente y las consecuencias derivadas de la exposición de los datos. No todas las filtraciones generan el mismo impacto jurídico; sin embargo, cuando se encuentran involucrados datos sensibles o biométricos, los riesgos para los derechos fundamentales aumentan considerablemente.

González (2007) sostiene que,

La protección de datos personales debe entenderse como un derecho fundamental propio del siglo XXI, debido a que el desarrollo tecnológico ha multiplicado las posibilidades de recopilación y tratamiento de información personal. Según el autor, las vulneraciones relacionadas con los datos personales afectan directamente la esfera individual de los ciudadanos y pueden comprometer elementos esenciales de su identidad, intimidad y dignidad. (p. 747).

La postura doctrinal expuesta permite comprender que una filtración de datos no constituye únicamente una falla técnica o administrativa. Detrás de cada registro comprometido existe una persona cuyos derechos pueden verse afectados mediante conductas como la suplantación de identidad, el fraude financiero, la discriminación, la extorsión, el daño reputacional o la exposición indebida de información privada.

De igual manera, Carrillo (2021) advierte que,

Uno de los principales problemas asociados al tratamiento de datos personales radica en el desconocimiento que poseen los titulares respecto de la forma en que su información es recopilada, utilizada y compartida. El autor señala que, en numerosos casos, los ciudadanos desconocen la finalidad específica del tratamiento de sus datos o los mecanismos mediante los cuales estos son utilizados por terceros. (p. 181).

Este criterio evidencia que la protección de datos personales requiere una actuación preventiva por parte de las instituciones responsables del tratamiento. No resulta suficiente obtener el consentimiento del titular para recopilar información; también es necesario garantizar que dicha información sea utilizada exclusivamente para las finalidades autorizadas y que permanezca protegida frente a accesos no autorizados.

Valor jurídico de los datos personales en la sociedad digital

En la actualidad, los datos personales constituyen un recurso estratégico para instituciones públicas y privadas, debido a su importancia en la prestación de servicios, gestión administrativa, salud, educación, seguridad y comercio electrónico. No obstante, su creciente utilización incrementa la responsabilidad de quienes los administran.

Los avances tecnológicos, mediante aplicaciones móviles, plataformas digitales, sistemas biométricos e inteligencia artificial, han permitido recopilar y procesar grandes volúmenes de información personal. Esta realidad exige que la protección de datos sea considerada un elemento esencial de la gestión institucional.

Desde una perspectiva constitucional, los datos personales no representan únicamente recursos informáticos o económicos, sino manifestaciones de la personalidad humana vinculadas con la dignidad y los derechos fundamentales. Por ello, su tratamiento inadecuado puede generar afectaciones a la privacidad, la seguridad y la autonomía individual, haciendo necesario que las instituciones adopten medidas preventivas para evitar vulneraciones.

Marco normativo

La protección de datos personales en Ecuador se fundamenta en la Constitución de la República y en la Ley Orgánica de Protección de Datos Personales, instrumentos que reconocen este derecho como una garantía vinculada con la privacidad, la dignidad humana y la autodeterminación informativa. La Constitución (2008), en su artículo 66 numeral 19, establece el derecho de las personas a acceder, controlar y decidir sobre la información que les concierne, exigiendo autorización del titular o mandato legal para su tratamiento.

La Ley Orgánica de Protección de Datos Personales desarrolla este derecho mediante principios como licitud, transparencia, finalidad, minimización, confidencialidad, seguridad

y responsabilidad proactiva, estableciendo obligaciones para instituciones públicas y privadas. Según Naranjo (2020), la ausencia inicial de una normativa específica limitó la aplicación efectiva de este derecho, evidenciando la necesidad de una regulación acorde con los desafíos de la transformación digital.

Asimismo, la normativa establece obligaciones frente a vulneraciones de seguridad, como la notificación a la Autoridad de Protección de Datos Personales, la comunicación a los titulares cuando exista riesgo para sus derechos y la implementación permanente de medidas técnicas, administrativas y organizativas de protección.

En este contexto, las acciones impulsadas por la Superintendencia de Protección de Datos Personales reflejan la importancia de fortalecer la prevención, supervisión y gestión de riesgos para garantizar una protección efectiva de la información personal en entornos digitales.

Responsabilidad jurídica de las instituciones públicas y privadas

La responsabilidad jurídica derivada de las filtraciones de datos personales debe analizarse desde una perspectiva integral, debido a que sus efectos pueden involucrar diferentes ámbitos del ordenamiento jurídico. Cuando una institución pública o privada recopila y trata información personal, asume el deber de garantizar su protección y responder por los daños ocasionados por una gestión negligente o ilícita.

La responsabilidad administrativa se configura cuando los responsables del tratamiento incumplen las obligaciones previstas en la Ley Orgánica de Protección de Datos Personales, como la falta de medidas de seguridad, la ausencia de notificación de vulneraciones o el tratamiento indebido de información. En estos casos, la autoridad competente puede imponer sanciones orientadas al cumplimiento normativo.

Asimismo, puede generarse responsabilidad civil cuando la filtración produce daños económicos, reputacionales, morales o afectaciones como suplantación de identidad y discriminación. La reparación integral procede cuando se demuestra el daño y la relación causal con la conducta institucional.

Además, las vulneraciones pueden adquirir dimensión constitucional al afectar derechos fundamentales como la privacidad y la autodeterminación informativa. En estos casos, mecanismos como el hábeas data permiten a los ciudadanos exigir la protección, actualización, rectificación o eliminación de sus datos.

En este sentido, la responsabilidad institucional no surge únicamente después de una filtración, sino desde el momento en que se recopila información personal. Por ello, el principio de responsabilidad proactiva exige adoptar medidas preventivas para reducir riesgos y garantizar una protección efectiva de los datos.

La Superintendencia de Protección de Datos Personales (2026) ha señalado que,

La gestión adecuada de riesgos constituye un elemento esencial dentro de los procesos de tratamiento de información personal. Para ello, las instituciones deben identificar amenazas, evaluar vulnerabilidades y adoptar medidas de mitigación que permitan reducir las probabilidades de afectación a los derechos de los titulares. (p.2).

Las filtraciones de datos personales pueden adquirir relevancia penal cuando las conductas involucradas se relacionan con acciones como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de comunicaciones, la divulgación indebida de información o la vulneración de la intimidad, generando responsabilidades según las circunstancias de cada caso.

En las instituciones públicas, esta responsabilidad adquiere especial importancia debido a la obligación constitucional del Estado de garantizar los derechos fundamentales. Las entidades estatales gestionan información sensible relacionada con salud, educación,

justicia, tributación y seguridad social, por lo que cualquier vulneración puede afectar gravemente a los ciudadanos y debilitar la confianza institucional.

De igual forma, las entidades privadas que recopilan y procesan datos personales, como instituciones financieras, educativas, sanitarias, empresas tecnológicas y plataformas digitales, deben implementar medidas adecuadas de protección y seguridad, considerando el volumen y la sensibilidad de la información que administran.

Las filtraciones de datos representan una amenaza significativa para derechos como la privacidad, la intimidad, la honra, la seguridad jurídica y la autodeterminación informativa. En este sentido, la responsabilidad jurídica de las instituciones no surge únicamente ante una vulneración, sino desde el momento en que asumen el tratamiento de información personal.

Por ello, toda entidad responsable del manejo de datos debe garantizar principios de legalidad, transparencia, seguridad y responsabilidad proactiva establecidos por el ordenamiento jurídico ecuatoriano. La protección de datos personales constituye, así, una garantía constitucional esencial frente a los riesgos derivados de la transformación digital.

El hábeas data como mecanismo de defensa frente a vulneraciones digitales

La creciente digitalización de las actividades humanas ha provocado que una cantidad significativa de información personal sea almacenada y procesada por instituciones públicas, empresas privadas y plataformas tecnológicas. En este contexto, la protección de los datos personales se ha convertido en una necesidad jurídica indispensable para garantizar el respeto de los derechos fundamentales. La posibilidad de acceder, corregir, actualizar o eliminar información personal constituye una garantía esencial para preservar la privacidad, la intimidad y la autodeterminación informativa de los ciudadanos frente a los riesgos derivados del tratamiento masivo de datos.

Dentro del sistema constitucional ecuatoriano, el hábeas data se configura como uno de los principales mecanismos de protección frente a vulneraciones relacionadas con el uso indebido de información personal. Esta garantía permite que los titulares de los datos ejerzan control sobre la información que les concierne y puedan exigir la tutela de sus derechos cuando estos resulten afectados por actuaciones de entidades públicas o privadas.

La importancia del hábeas data ha aumentado significativamente en la era digital. Actualmente, los datos personales ya no se encuentran únicamente en archivos físicos o registros administrativos tradicionales, sino también en redes sociales, plataformas digitales, aplicaciones móviles, sistemas biométricos y bases de datos automatizadas. Como consecuencia, los riesgos asociados a la pérdida de control sobre la información personal se han incrementado, haciendo necesaria la existencia de mecanismos constitucionales eficaces que permitan a los ciudadanos defender sus derechos.

Fundamentos teóricos del hábeas data

El hábeas data constituye una garantía jurisdiccional destinada a proteger los derechos relacionados con el acceso, conocimiento, actualización, rectificación, eliminación y protección de datos personales. Su finalidad principal consiste en garantizar que toda persona conserve el control sobre la información que le concierne y pueda defenderse frente a usos indebidos o ilegítimos de sus datos.

En Ecuador, esta garantía se encuentra reconocida en el artículo 92 de la Constitución de la República, el cual establece que toda persona podrá acceder a los documentos, bancos o archivos de datos personales e informes que sobre ella consten en entidades públicas o privadas. Asimismo, la norma reconoce el derecho a conocer el uso y finalidad de dicha

información, así como a solicitar su actualización, rectificación, eliminación o anulación cuando corresponda.

Desde una perspectiva constitucional, el hábeas data constituye una manifestación práctica del derecho a la autodeterminación informativa. No se limita únicamente a permitir el acceso a la información, sino que reconoce a los ciudadanos la facultad de intervenir activamente en las decisiones relacionadas con el tratamiento de sus datos personales.

La importancia de esta garantía radica en que permite equilibrar la relación entre el titular de la información y las instituciones que administran bases de datos. Sin mecanismos de control como el hábeas data, los ciudadanos quedarían en una posición de vulnerabilidad frente al poder que poseen las entidades capaces de recopilar, almacenar y procesar grandes cantidades de información personal.

Hábeas data como garantía de control sobre la información personal

El verdadero alcance del hábeas data trasciende la simple consulta de documentos o registros. Su función principal consiste en garantizar que las personas puedan ejercer control efectivo sobre la información relacionada con su identidad, trayectoria personal y actividades cotidianas.

En este sentido, De la Cueva (2008) sostiene que, Mientras el derecho a la intimidad protege a las personas frente a intromisiones indebidas en su vida privada, el derecho a la protección de datos tiene como finalidad otorgar a los individuos un poder de control sobre el uso y destino de su información personal. Esta diferenciación resulta fundamental porque permite comprender que la protección de datos constituye un derecho autónomo con finalidades específicas. (pp.34-36).

La postura doctrinal expuesta evidencia que el hábeas data se convierte en la herramienta procesal mediante la cual la autodeterminación informativa adquiere eficacia práctica. Gracias a esta garantía, el ciudadano puede conocer quién posee sus datos, para qué los utiliza, durante cuánto tiempo los conserva y si han sido compartidos con terceros.

Esta facultad resulta especialmente relevante en una sociedad caracterizada por la utilización intensiva de tecnologías digitales. Actualmente, las personas entregan información personal para acceder a servicios bancarios, educativos, sanitarios, laborales y comerciales, muchas veces sin conocer completamente el destino de dicha información. El hábeas data permite reducir esta asimetría y fortalecer la posición jurídica del titular frente a quienes administran sus datos.

Hábeas data frente a redes sociales y difusión no consentida de información

Uno de los principales desafíos contemporáneos para la protección de datos personales se relaciona con la difusión no autorizada de imágenes, videos, fotografías, audios y demás contenidos digitales que permiten identificar a una persona. Este fenómeno se ha intensificado debido al uso masivo de redes sociales y plataformas digitales capaces de multiplicar el alcance de cualquier publicación en cuestión de segundos.

La divulgación no consentida de información personal puede generar graves afectaciones a la honra, intimidad, reputación, estabilidad emocional y dignidad de las personas. En muchos casos, el daño ocasionado resulta difícil de reparar debido a la velocidad con la que la información puede replicarse en entornos digitales.

La jurisprudencia constitucional ecuatoriana ha reconocido esta problemática. En la Sentencia No. 2064-14-EP/21, la Corte Constitucional analizó un caso relacionado con la difusión de fotografías íntimas sin consentimiento de la titular. En dicha decisión, el máximo

órgano de control constitucional destacó la relevancia del hábeas data como mecanismo de protección frente a vulneraciones que afectan directamente la privacidad y la dignidad de las personas en entornos digitales.

Esta sentencia representa un avance significativo en la interpretación constitucional del hábeas data, debido a que amplía su ámbito de aplicación más allá de los registros documentales tradicionales y reconoce su utilidad frente a nuevas formas de vulneración derivadas del uso de tecnologías digitales.

Hábeas data y autodeterminación informativa

La autodeterminación informativa constituye uno de los fundamentos esenciales del derecho a la protección de datos personales. Este principio reconoce que toda persona debe conservar la capacidad de decidir sobre el tratamiento de la información que le concierne y participar activamente en las decisiones relacionadas con el uso de sus datos.

Mendoza (2014) sostiene que,

Los datos personales forman parte de la esfera privada e íntima de los individuos, debido a que permiten identificarlos y diferenciarlos dentro de la sociedad. Asimismo, señala que la protección de esta información implica reconocer derechos específicos relacionados con el acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales. (p.5).

La importancia de esta postura radica en que permite comprender que el control de la información personal constituye una condición indispensable para el ejercicio de otros derechos fundamentales. Cuando una persona pierde la capacidad de decidir sobre sus datos, también disminuye su autonomía frente a quienes administran dicha información.

En consecuencia, el hábeas data se configura como el instrumento jurídico que permite materializar la autodeterminación informativa. Gracias a esta garantía, los ciudadanos pueden ejercer un control efectivo sobre sus datos personales y exigir que las instituciones respeten los principios de legalidad, transparencia y finalidad que deben regir todo tratamiento de información.

El hábeas data constituye una garantía constitucional indispensable para la protección de los datos personales en la sociedad digital contemporánea. Su importancia radica en que permite a los ciudadanos conservar el control sobre la información que les concierne y defenderse frente a usos indebidos, tratamientos ilegítimos o vulneraciones derivadas de la gestión inadecuada de datos personales.

El análisis desarrollado evidencia que esta garantía trasciende la simple consulta de información, convirtiéndose en un mecanismo efectivo para proteger la privacidad, la intimidad, la honra, la autodeterminación informativa y la dignidad humana. Asimismo, la jurisprudencia constitucional ecuatoriana ha demostrado que el hábeas data posee la capacidad de adaptarse a los desafíos planteados por la transformación digital y responder a nuevas formas de vulneración que afectan a los ciudadanos en entornos tecnológicos.

Por ello, el fortalecimiento de esta garantía resulta fundamental para asegurar que el desarrollo tecnológico se produzca dentro de un marco de respeto a los derechos fundamentales. En una sociedad donde la información constituye uno de los recursos más valiosos, el hábeas data se convierte en una herramienta esencial para preservar la libertad y autonomía de las personas frente al creciente poder de quienes administran datos personales.

Jurisprudencia internacional sobre protección de datos personales y derechos fundamentales

La protección de los datos personales ha experimentado una importante evolución a través de la jurisprudencia internacional, particularmente en aquellos casos en los que los tribunales han debido pronunciarse sobre el alcance del derecho a la vida privada frente a las nuevas formas de tratamiento y circulación de información. Estas decisiones han contribuido a consolidar criterios jurídicos que actualmente sirven de fundamento para la regulación de la protección de datos personales en diversos ordenamientos jurídicos.

La jurisprudencia internacional ha reconocido que la protección de los datos personales constituye una manifestación directa del derecho a la vida privada y de la dignidad humana. Asimismo, ha señalado que los Estados tienen la obligación de adoptar medidas adecuadas para prevenir injerencias arbitrarias en la esfera personal de los individuos, especialmente cuando estas se producen mediante el uso de tecnologías de información y comunicación.

El caso Escher y otros vs. Brasil: protección de la vida privada frente a la vigilancia estatal

Uno de los precedentes más relevantes en materia de privacidad y protección de datos personales es el caso Escher y otros vs. Brasil, resuelto por la Corte Interamericana de Derechos Humanos en 2009.

En esta sentencia, la Corte Interamericana de Derechos Humanos (2009) analizó la interceptación y divulgación de comunicaciones telefónicas realizadas por autoridades estatales sin las debidas garantías jurídicas. El tribunal concluyó que dichas actuaciones vulneraron el derecho a la vida privada reconocido en el artículo 11 de la Convención Americana sobre Derechos Humanos, al considerar que las comunicaciones privadas forman parte de la esfera de protección de la intimidad de las personas.

La Corte Interamericana de Derechos Humanos (2009) sostuvo que la protección de la vida privada no se limita al contenido de las comunicaciones, sino que comprende toda información vinculada con la actividad personal de los individuos, incluyendo registros, datos y demás elementos que permitan conocer aspectos de su vida privada. Asimismo, estableció que cualquier intervención estatal sobre este tipo de información debe cumplir estrictamente los principios de legalidad, necesidad y proporcionalidad.

Este criterio resulta especialmente relevante en la actualidad debido a que demuestra que la recopilación y tratamiento de datos personales pueden constituir una forma de injerencia en la vida privada cuando no existen garantías adecuadas para proteger los derechos de los ciudadanos. En consecuencia, la sentencia refuerza la necesidad de que los Estados adopten mecanismos eficaces para regular el tratamiento de información personal y prevenir prácticas de vigilancia incompatibles con los derechos humanos.

La Sentencia del Censo de Alemania y el reconocimiento de la autodeterminación informativa

Uno de los precedentes más relevantes en materia de protección de datos personales es la Sentencia del Censo (Volkszählungsurteil), emitida por el Tribunal Constitucional Federal de Alemania en 1983. En esta decisión, el Tribunal analizó la constitucionalidad de la Ley del Censo y desarrolló el concepto de autodeterminación informativa (informationelle Selbstbestimmung), entendido como el derecho de las personas a decidir sobre la divulgación, uso y tratamiento de los datos que les conciernen.

El Tribunal Constitucional Federal Alemán (1983) estableció que una sociedad democrática no puede garantizar plenamente la libertad individual si los ciudadanos desconocen quién recopila su información, qué datos son almacenados y con qué finalidad serán utilizados. La falta de control sobre los datos personales puede afectar el libre desarrollo de la personalidad y limitar indirectamente el ejercicio de otros derechos fundamentales

La importancia de esta sentencia radica en que estableció las bases del moderno derecho a la protección de datos personales, influyendo en legislaciones nacionales e instrumentos internacionales posteriores. Sus principios consolidaron la idea de que la información personal no constituye únicamente un elemento de privacidad, sino un ámbito donde las personas deben conservar capacidad de decisión y control.

Los precedentes internacionales analizados evidencian que la protección de datos personales ha evolucionado desde una visión tradicional de privacidad hacia el reconocimiento de un derecho fundamental autónomo. Tanto la Corte Interamericana de Derechos Humanos como el Tribunal Constitucional Federal Alemán coinciden en que las personas deben mantener control sobre la información que les pertenece y que cualquier tratamiento de datos debe estar sujeto a principios de legalidad, proporcionalidad y justificación.

En este sentido, la jurisprudencia internacional proporciona criterios esenciales para fortalecer la interpretación y aplicación de las garantías reconocidas en el ordenamiento jurídico ecuatoriano, especialmente frente a los desafíos derivados del tratamiento masivo de información personal en los entornos digitales contemporáneos.

DISCUSIÓN

El análisis realizado evidencia que la protección de los datos personales se ha consolidado como un derecho fundamental autónomo, estrechamente vinculado con la dignidad humana, la privacidad y la autodeterminación informativa. La transformación digital ha propiciado nuevas formas de recopilación, almacenamiento y tratamiento de información personal que, aunque favorecen el desarrollo de múltiples actividades sociales, económicas y administrativas, también incrementan los riesgos de vulneración de derechos fundamentales. En este contexto, la protección jurídica de los datos personales adquiere una importancia creciente dentro de los Estados constitucionales.

Los resultados muestran que el ordenamiento jurídico ecuatoriano dispone de un marco normativo sólido para la protección de este derecho. La Constitución de la República del Ecuador reconoce expresamente la protección de los datos personales, mientras que la Ley Orgánica de Protección de Datos Personales desarrolla principios, obligaciones y mecanismos destinados a regular el tratamiento de la información personal. Estas disposiciones proporcionan herramientas jurídicas que permiten garantizar el control de los ciudadanos sobre los datos que les conciernen

Sin embargo, el reconocimiento normativo resulta insuficiente si no se acompaña de una aplicación efectiva. El análisis de las filtraciones de datos personales evidencia que continúan produciéndose vulneraciones tanto en instituciones públicas como privadas, con afectaciones a la privacidad, la seguridad y la dignidad de las personas. En consecuencia, la eficacia del sistema depende no solo de la existencia de normas, sino también de su cumplimiento, supervisión y aplicación por parte de los responsables del tratamiento de datos.

Asimismo, el estudio del hábeas data demuestra que el sistema constitucional ecuatoriano cuenta con un mecanismo jurisdiccional eficaz para garantizar la autodeterminación informativa, al permitir que los titulares accedan, rectifiquen, actualicen,

eliminen o protejan la información relacionada con su persona cuando esta sea objeto de tratamientos ilegítimos. La jurisprudencia constitucional ha mostrado una tendencia favorable a adaptar esta garantía a los desafíos propios de los entornos digitales.

El análisis comparado confirma esta perspectiva. Tanto la Corte Interamericana de Derechos Humanos como el Tribunal Constitucional Federal Alemán han reconocido que el control sobre la información personal constituye un presupuesto indispensable para el ejercicio de los derechos y libertades fundamentales, fortaleciendo la concepción de la protección de datos personales como un derecho autónomo.

En síntesis, los mecanismos jurídicos y constitucionales vigentes en Ecuador proporcionan una base adecuada para proteger los derechos fundamentales frente al tratamiento masivo de datos personales. No obstante, su eficacia práctica requiere fortalecer la cultura de protección de datos, consolidar los mecanismos de supervisión y asegurar el cumplimiento efectivo de las obligaciones legales por parte de las instituciones. Solo mediante una acción coordinada entre el Estado, los responsables del tratamiento y la ciudadanía será posible garantizar un equilibrio entre el desarrollo tecnológico y la protección efectiva de los derechos fundamentales.

CONCLUSIONES

La protección de los datos personales constituye un derecho fundamental autónomo sustentado en la dignidad humana, la privacidad y la autodeterminación informativa. En el contexto del uso masivo de tecnologías digitales, su garantía resulta indispensable para preservar los derechos fundamentales de las personas frente al tratamiento continuo de información personal.

El ordenamiento jurídico ecuatoriano cuenta con un marco constitucional y legal que reconoce y regula este derecho, especialmente mediante la Constitución de la República y la Ley Orgánica de Protección de Datos Personales. Asimismo, el hábeas data se consolida como un mecanismo jurisdiccional eficaz para que los titulares ejerzan control sobre su información y exijan su corrección, actualización, eliminación o protección cuando existan tratamientos ilegítimos.

Aunque Ecuador dispone de mecanismos jurídicos adecuados para proteger los datos personales, persisten desafíos relacionados con las filtraciones de información y las nuevas formas de tratamiento masivo de datos. En consecuencia, la eficacia de este sistema depende del fortalecimiento de la cultura de protección de datos, del cumplimiento efectivo de las obligaciones legales por parte de las instituciones y de una supervisión estatal capaz de responder a los retos de los entornos digitales contemporáneos.

REFERENCIAS BIBLIOGRÁFICAS

- Carrillo, J. (2021). Protección de datos personales y desafíos jurídicos en entornos digitales. *Revista Jurídica Contemporánea*, 12(2), 45-62. <https://acortar.link/SlobZE>
- Constitución de la República del Ecuador. (2008). Registro Oficial No. 449 de 20 de octubre de 2008. <https://acortar.link/u2Y3J>
- Corte Interamericana de Derechos Humanos. (2009). Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (Excepciones preliminares, fondo, reparaciones y costas). <https://www.corteidh.or.cr>
- Corte Constitucional del Ecuador. (2021). Sentencia No. 2064-14-EP/21. <https://www.corteconstitucional.gob.ec>
- De la Cueva, P. (2008). La protección de datos personales y la autodeterminación informativa. Editorial Jurídica. <https://acortar.link/kmPQp7>

- González, M. (2007). La protección de datos personales como derecho fundamental en la sociedad de la información. *Revista de Derecho y Nuevas Tecnologías*, 4(1), 2-36. <https://acortar.link/LDZHZ8>
- Ley Orgánica de Protección de Datos Personales. (2021). Registro Oficial Suplemento No. 459 de 26 de mayo de 2021. <https://acortar.link/rLsOP2>
- Loja, A. (2020). Privacidad y protección de datos personales en la era digital. *Revista Latinoamericana de Derecho Informático*, 8(1), 55-74. <https://acortar.link/jumvh4>
- Mata, F. (2015). Dignidad humana y derechos fundamentales: fundamentos para su protección jurídica. *Revista Ius*, 9(2), 15-32. <https://acortar.link/HwWiML>
- Mendoza, R. (2014). La autodeterminación informativa como garantía de los derechos fundamentales. *Revista Iberoamericana de Derecho Constitucional*, 6(1), 77-95. <https://acortar.link/WVs6dr>
- Naranjo, D. (2020). Situación De La Protección De Datos Personales En Ecuador. *Revista Jurídica de Investigación e Innovación*, 5(2), 101-118. <https://acortar.link/qTkQIk>
- Ronál, F. (2021). Autodeterminación informativa y protección de datos personales en Ecuador. *Revista Ecuatoriana de Derecho Constitucional*, 7(1), 35-58. <https://acortar.link/NIRv7r>
- Pfeffer, E. (2015). Los derechos a la intimidad, vida privada, honra e imagen en el constitucionalismo contemporáneo. *Revista de Derecho Público*, 83, 125-148. <https://acortar.link/Pg5qAo>
- Tribunal Constitucional Federal Alemán. (1983). Sentencia del Censo (Volkszählungsurteil), BVerfGE 65, 1, de 15 de diciembre de 1983. Karlsruhe, Alemania.
- Vaca, J. (2026). Protección de datos personales y garantías constitucionales en Ecuador. *Revista Jurídica Ecuatoriana*, 14(1), 67-89. <https://acortar.link/bozii3>



Esta obra está bajo una licencia internacional [Creative Commons Atribución-NoComercial-CompartirIgual 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Copyright: La Fundación Internacional para la Educación la Ciencia y la Tecnologías, "FIECYT" conserva los derechos patrimoniales (copyright) de los artículos publicados, y favorece y permite la reutilización de las mismas bajo la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Ecuador. Se pueden copiar, usar, difundir, transmitir y exponer públicamente, siempre que: se cite la autoría y la fuente original de su publicación (revista, editorial y URL de la obra); no se usen para fines comerciales; se mencione la existencia y especificaciones de esta licencia de uso.

Autoría: En la lista de autores firmantes deben figurar únicamente aquellas personas que han contribuido intelectualmente al desarrollo del trabajo. Haber colaborado en la recolección de datos no es, por sí mismo, criterio suficiente de autoría. "KIRIA" declina cualquier responsabilidad sobre posibles conflictos derivados de la autoría de los trabajos que se publiquen.