

Vol. 1, No. 6 (setembro 2026)

REVISTA ATHENA LATINHO-AMERICANA

PROTECCIÓN DE DATOS PERSONALES COMO BIEN JURÍDICO PROTEGIDO

Protection of Personal Data as a Protected Legal Interest

Juan Carlos Illescas Navarrete¹

Revista Athena Latino-Americana

DOI: 10.69720/3086-5182.2026.000070

ISSN: [3086-5182](https://issn.org/3086-5182)

¹Licenciado en ciencias publicas y sociales, dr en jurisprudencia y abogado de los tribunales de la república, especialista superior en derecho administrativo, magister en derecho administrativo, magister en administración pública mencion gestión por resultados, magister en derecho procesal constitucional, maestría de la maestría en derecho laboral público y privado de la u central del Ecuador

ORCID: <https://orcid.org/0009-0002-5525-4043>

E-mail: juan_k_illescas@hotmail.com



PROTECCIÓN DE DATOS PERSONALES COMO BIEN JURÍDICO PROTEGIDO

Juan Carlos Illescas Navarrete



PERIÓDICO CIENTÍFICO INDEXADO INTERNACIONALMENTE

ISSN
International Standard Serial Number
3086-5182
www.athena-latino-americana.com

Editora e Revista
Athena Latino-Americana
CPF: 639.619.621-20
Naviraí – Mato Grosso do Sul
Rua: Botocudos, 365 – Centro
CEP: 79950-000

RESUMO

A proteção de dados pessoais constitui um direito fundamental relacionado à dignidade humana, à liberdade, à privacidade e ao livre desenvolvimento da personalidade. Com a expansão das tecnologias digitais, a coleta, o armazenamento e o processamento de informações pessoais passaram a ocorrer em grande escala, aumentando benefícios sociais e econômicos, mas também riscos de vigilância, perfilamento, discriminação e perda de controle sobre os dados. O estudo analisa a proteção de dados pessoais como bem jurídico protegido no ordenamento jurídico equatoriano, destacando sua autonomia em relação ao direito à intimidade e sua relação com a autodeterminação informativa. Examina-se o poder do titular de conhecer, decidir e controlar o tratamento de suas informações, bem como os princípios, direitos, obrigações e mecanismos de tutela previstos na Constituição da República do Equador, na Lei Orgânica de Proteção de Dados Pessoais e em seu Regulamento Geral. Também são abordados os desafios decorrentes do tratamento massivo de dados e do uso de sistemas de inteligência artificial, ressaltando a necessidade de transparência, segurança, proporcionalidade, responsabilidade e supervisão. Conclui-se que a proteção de dados deve colocar a pessoa no centro das decisões relacionadas ao tratamento de suas informações, garantindo o respeito aos direitos fundamentais diante da transformação digital.

Palavras-chave: Proteção de dados pessoais; Direito fundamental; Autodeterminação informativa; Privacidade; Inteligência artificial; Ordenamento jurídico equatoriano.

ABSTRACT

Personal data protection constitutes a fundamental right linked to human dignity, liberty, privacy, and the free development of personality. With the expansion of digital technologies, the collection, storage, and processing of personal information have occurred on a large scale, increasing social and economic benefits but also raising risks regarding surveillance, profiling, discrimination, and the loss of control over data. This study analyzes personal data protection as a protected legal interest within the Ecuadorian legal system, highlighting its autonomy from the right to privacy and its relationship with informational self-determination. It examines the data subject's power to know about, decide on, and control the processing of their information, as well as the principles, rights, obligations, and protection mechanisms established in the Constitution of the Republic of Ecuador, the Organic Law on Personal Data Protection, and its General Regulations. Challenges arising from mass data processing and the use of artificial intelligence systems are also addressed, emphasizing the need for transparency, security, proportionality, accountability, and oversight. The study concludes that data protection must place the individual at the center of decisions regarding the processing of their information, ensuring respect for fundamental rights in the face of digital transformation.

Keywords: Personal data protection; Fundamental right; Informational self-determination; Privacy; Artificial intelligence; Ecuadorian legal system.

1. INTRODUÇÃO

La expansión de las tecnologías digitales ha convertido a los datos personales en un insumo permanente de la actividad pública y privada. La identidad, los desplazamientos, las preferencias, la salud, las comunicaciones y las interacciones cotidianas pueden ser registrados, relacionados y analizados a una escala antes impensable. Esta realidad ha generado beneficios sociales y económicos, pero también nuevas formas de vigilancia, perfilamiento, discriminación y pérdida de control sobre la información personal. Como advierte Morales (2019), en el entorno digital «estamos abriendo ventanas de miles de maneras para que se asomen a nuestra intimidad virtual» (p. 38).

En este contexto, la protección de datos personales puede ser examinada como un bien jurídico protegido: un interés esencial para la dignidad, la libertad y el libre desarrollo de la

personalidad, reconocido por el ordenamiento

jurídico y dotado de mecanismos de garantía. No se protege el dato como un objeto aislado o con valor autónomo, sino la posición jurídica de la persona a la que la información se refiere. El núcleo de la tutela radica en evitar que la recopilación y el uso de información personal conviertan al individuo en un sujeto transparente, susceptible de ser observado, clasificado o condicionado sin conocimiento, justificación o posibilidades reales de intervención.

El presente artículo analiza la protección de datos personales como bien jurídico protegido, a partir de su evolución doctrinal y de su configuración en el ordenamiento ecuatoriano. Para ello, se examinan su autonomía respecto de la intimidad, su relación con la autodeterminación informativa, el contenido del poder de control

reconocido al titular y la función de los principios, derechos, obligaciones y mecanismos de tutela previstos en la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD) y su Reglamento General. Finalmente, se consideran los desafíos derivados del tratamiento masivo de datos y del uso de inteligencia artificial.

2. DESAROLLO

1. De la intimidad a un derecho fundamental autónomo

La protección de datos surgió históricamente vinculada a la intimidad. La preocupación inicial se concentró en impedir injerencias indebidas en la esfera privada, especialmente ante la capacidad de los sistemas informáticos para almacenar, recuperar y relacionar grandes volúmenes de información. Ayjón (2020a) explica que la necesidad de regulación apareció cuando se constató «la gran capacidad de las computadoras para almacenar datos e información» (p. 470) y los riesgos asociados con su tratamiento inadecuado.

Sin embargo, la evolución tecnológica evidenció que limitar la tutela a los datos íntimos era insuficiente. Un dato aparentemente neutro —como la ubicación, un identificador, el historial de navegación o el uso de una tarjeta de transporte— puede adquirir un significado sensible cuando se combina con otros datos, se analiza en el tiempo o se emplea para adoptar decisiones sobre una persona. Por ello, el ámbito protegido se desplazó desde el secreto o la reserva hacia el control de cualquier información vinculada con una persona identificada o identificable.

Esta evolución permitió reconocer la protección de datos como un derecho autónomo. Trujillo Cabrera y Lorenzo Cabrera (2021) sostienen que su objeto «no se reduce solo a los datos íntimos de la persona» (p. 94), sino que se extiende a cualquier dato personal cuyo conocimiento o utilización por terceros pueda afectar sus derechos. En la misma línea, Ayjón (2020b) señala que se trata de un derecho «autónomo, independiente, diferenciado del derecho a la intimidad» (p. 134).

La distinción no implica una ruptura absoluta entre ambos derechos. La intimidad continúa siendo uno de los intereses que puede resultar afectado por el tratamiento de datos; no obstante, la protección de datos ofrece una tutela más amplia y dinámica. Mientras la intimidad se relaciona principalmente con la preservación de un ámbito reservado frente a injerencias, la protección de datos regula todo el

ciclo de vida de la información personal, incluso cuando esta no sea secreta o haya sido obtenida legítimamente. En consecuencia, la lesión no depende únicamente de que se revele un dato íntimo: también puede producirse por recopilar datos sin base jurídica, reutilizarlos para fines incompatibles, conservarlos de manera excesiva, mantenerlos inexactos, comunicarlos indebidamente o impedir al titular ejercer sus derechos.

2. La persona, y no el dato, como centro de la tutela

Considerar la protección de datos como bien jurídico exige identificar correctamente el objeto de tutela. Los datos son representaciones de características, conductas o circunstancias de una persona; por tanto, su protección es instrumental respecto de la dignidad, la libertad, la igualdad y el desarrollo de la personalidad. El ordenamiento no pretende inmovilizar la información ni establecer un dominio patrimonial absoluto del titular sobre ella. Busca asegurar que el tratamiento se realice dentro de límites jurídicos que preserven la capacidad de la persona para conocer, intervenir y exigir responsabilidad.

La Constitución ecuatoriana reconoce expresamente esta dimensión en el artículo 66, numeral 19, al garantizar «el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter» (Constitución de la República del Ecuador, 2008, art. 66.19). La referencia conjunta al acceso y a la decisión revela que el contenido constitucional no se agota en la confidencialidad. Comprende una facultad activa de intervención del titular sobre el tratamiento de su información.

La LOPDP desarrolla esta garantía y define como su objeto «garantizar el ejercicio del derecho a la protección de datos personales» (Ley Orgánica de Protección de Datos Personales, 2021, art. 1). A su vez, el Reglamento General establece que su finalidad es desarrollar la normativa aplicable y proteger «los derechos y libertades fundamentales de los titulares de datos personales» (Reglamento General de la Ley Orgánica de Protección de Datos Personales, 2023, art. 1). Estas disposiciones confirman que el dato no constituye el fin último de la regulación: la protección se dirige a la persona y a las consecuencias que el tratamiento puede producir sobre sus derechos y libertades.

Esta precisión es relevante porque evita identificar la tutela con una obligación absoluta

de secreto. Los datos personales pueden ser tratados legítimamente cuando existe una base jurídica y se respetan los principios aplicables. Lo jurídicamente protegido es la posición del titular frente al tratamiento: su derecho a recibir información, acceder, rectificar, actualizar, eliminar, oponerse o solicitar la suspensión, según corresponda; y su expectativa de que responsables y encargados actúen de manera lícita, leal, transparente, segura y responsable.

3. Autodeterminación informativa y poder de control

La autodeterminación informativa permite explicar el contenido esencial del bien jurídico. Esta noción alude a la capacidad de la persona para conocer y participar en las decisiones relativas al uso de sus datos. No supone que todo tratamiento dependa del consentimiento, pues la ley reconoce otras bases de legitimación; significa que ningún tratamiento puede situarse fuera de controles, finalidades y garantías previamente definidos.

Ayón (2020b) sintetiza este contenido al afirmar que el derecho atribuye «un poder de disposición y control sobre los datos personales» (p. 136). De manera concordante, Trujillo Cabrera y Lorenzo Cabrera (2021) ubican su contenido nuclear en el poder del titular para decidir qué información proporcionar, conocer quién la posee, determinar para qué se utiliza y oponerse cuando corresponda (p. 94). Desde esta perspectiva, el bien jurídico protegido puede formularse como el derecho fundamental de la persona a conservar un ámbito efectivo de conocimiento, decisión y control sobre el tratamiento de la información que le concierne.

El poder de control se materializa en garantías concretas. Primero, la persona debe ser informada de manera clara y oportuna sobre la identidad del responsable, las finalidades, la base de legitimación, el tiempo de conservación, las transferencias y la forma de ejercer sus derechos. Segundo, el tratamiento debe responder a fines determinados y compatibles; la obtención lícita de datos para una finalidad no autoriza automáticamente su utilización posterior para objetivos distintos. Tercero, deben tratarse únicamente los datos adecuados, pertinentes y necesarios. Cuarto, el responsable debe garantizar su exactitud, seguridad y conservación limitada. Finalmente, el titular debe contar con vías administrativas y judiciales eficaces para restablecer el control perdido y obtener reparación.

La acción de hábeas data prevista en el artículo 92 de la Constitución expresa esta

dimensión garantista. La persona puede conocer la existencia de archivos o bancos de datos, acceder a ellos, conocer su uso, finalidad, origen, destino y vigencia, y solicitar su actualización, rectificación, eliminación o anulación (Constitución de la República del Ecuador, 2008, art. 92). Así, la protección constitucional no es únicamente declarativa: incorpora un mecanismo jurisdiccional orientado a hacer efectivo el control del titular.

4. Principios y deberes como estructura de protección

La tutela del bien jurídico no depende únicamente del ejercicio reactivo de derechos. La LOPDP configura un sistema preventivo mediante principios y obligaciones que condicionan la legitimidad del tratamiento desde su diseño. Los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación, seguridad y responsabilidad proactiva delimitan la conducta de responsables y encargados.

La finalidad cumple una función central: impide que los datos sean recogidos bajo una justificación y utilizados posteriormente con otra incompatible. La minimización y la proporcionalidad evitan la recopilación excesiva. La transparencia reduce las asimetrías de información entre la organización y el titular. La seguridad protege frente a pérdida, alteración, divulgación o acceso no autorizado. La responsabilidad proactiva exige, además, que quien trata datos no solo cumpla la normativa, sino que pueda demostrarlo mediante políticas, registros, análisis de riesgos, evaluaciones de impacto, medidas técnicas y organizativas y procedimientos de atención de derechos.

Estas garantías muestran que la protección de datos es un bien jurídico de naturaleza transversal. Una infracción puede afectar simultáneamente la intimidad, la igualdad, la honra, la libertad de expresión, el trabajo, la educación o el debido proceso. Por ejemplo, un perfil inexacto puede excluir a una persona de un servicio; un sistema de vigilancia desproporcionado puede condicionar su conducta; y una decisión automatizada opaca puede impedirle comprender o controvertir el resultado. La protección de datos opera, por ello, como presupuesto para el ejercicio de otros derechos en sociedades intensivas en información.

La organización institucional también forma parte de esta estructura protectora. El

Libro blanco del DPO destaca que la protección de datos ha adquirido «una dimensión estratégica» en la gestión de la privacidad y del cumplimiento (ISMS Forum, 2025, p. 8). El delegado de protección de datos, cuando sea exigible, contribuye con asesoramiento y supervisión independiente; sin embargo, la responsabilidad de determinar los fines y medios del tratamiento, implementar medidas y demostrar cumplimiento permanece en el responsable. La existencia de una función especializada no desplaza la obligación institucional de proteger el bien jurídico.

5. Riesgos contemporáneos: tratamiento masivo e inteligencia artificial

La protección del bien jurídico enfrenta desafíos crecientes por la capacidad de inferencia de los sistemas digitales. El riesgo ya no se limita a la divulgación de información almacenada. Los modelos analíticos pueden deducir atributos, anticipar comportamientos, clasificar personas y generar decisiones a partir de datos obtenidos en contextos diversos. Además, la concentración de información incrementa las consecuencias de fallas de seguridad y facilita usos secundarios difícilmente previsibles para el titular.

La inteligencia artificial intensifica estos riesgos cuando utiliza datos personales para entrenamiento, generación de perfiles o apoyo a decisiones. En el ámbito judicial, por ejemplo, la UNESCO (2026) recomienda adoptar y utilizar sistemas que protejan la privacidad y eviten riesgos de divulgación o acceso no autorizado (p. 32). Aunque estas directrices se dirigen a cortes y tribunales, expresan un criterio aplicable a cualquier organización: la innovación tecnológica debe someterse a los derechos fundamentales y no convertirse en una justificación para reducir las garantías.

La protección efectiva requiere evaluar la necesidad y proporcionalidad del tratamiento antes de implementarlo, identificar los grupos potencialmente afectados, asegurar la calidad de los datos, limitar accesos, documentar decisiones y establecer supervisión humana. Cuando el tratamiento pueda entrañar un alto riesgo, la evaluación de impacto permite anticipar afectaciones y definir salvaguardas. En sistemas automatizados, la transparencia debe incluir información significativa sobre la lógica, los criterios utilizados y las consecuencias previstas, sin perjuicio de la protección de secretos legítimos.

En este escenario, concebir la

protección de datos como bien jurídico protegido tiene una consecuencia práctica: obliga a evaluar los tratamientos desde la afectación posible a la persona, y no únicamente desde la utilidad de la tecnología o la seguridad del sistema. Un tratamiento puede ser técnicamente seguro y, al mismo tiempo, resultar ilícito, desproporcionado, discriminatorio o incompatible con la finalidad informada. La seguridad es una condición necesaria, pero no suficiente, para la licitud.

6. Alcance de la expresión «bien jurídico protegido»

En sentido amplio, un bien jurídico es un interés o valor relevante para la convivencia y el desarrollo de la persona que el ordenamiento reconoce y tutela. En materia de datos personales, la expresión resulta adecuada siempre que no se confunda el soporte informacional con el verdadero objeto de protección. El bien jurídico no es el dato considerado aisladamente ni un supuesto derecho de propiedad sobre la información. Es el derecho fundamental de la persona a que el tratamiento de sus datos respete su dignidad, sus libertades y su capacidad de control.

Esta formulación también permite reconocer una dimensión individual y otra institucional. En el plano individual, protege a cada titular frente a tratamientos que reduzcan injustificadamente su autonomía o afecten sus derechos. En el plano institucional, exige reglas de gobernanza, autoridades de control, mecanismos de reclamación y una cultura de responsabilidad que preserve la confianza en los ecosistemas digitales. La tutela no se limita, por tanto, a reparar daños consumados; busca prevenir tratamientos capaces de crear riesgos indebidos.

En conclusión, la protección de datos personales constituye un bien jurídico autónomo y de naturaleza fundamental, estrechamente relacionado con la dignidad humana y funcionalmente conectado con otros derechos. Su contenido esencial se manifiesta en el poder de conocimiento, decisión y control del titular; su protección se concreta mediante principios, derechos, obligaciones preventivas, supervisión y mecanismos de tutela. En Ecuador, los artículos 66, numeral 19, y 92 de la Constitución, junto con la LOPDP y su Reglamento General, proporcionan una base normativa suficiente para afirmar que toda actividad de tratamiento debe situar a la persona en el centro. Esta comprensión resulta indispensable para enfrentar los riesgos del tratamiento masivo y de la inteligencia artificial

sin renunciar a la innovación, pero subordinándola al respeto efectivo de los derechos fundamentales.

3. REFERENCIAS

Ayón, M. M. (2020a). Antecedentes y evolución histórica del delito contra la protección de datos de carácter personal. En La protección de datos de carácter personal en la justicia penal (pp. 469–506). J. M. Bosch. <https://www.jstor.org/stable/j.ctv14t46p2.12>

Ayón, M. M. (2020b). Cuestiones fundamentales en el derecho a la protección de los datos de carácter personal. En La protección de datos de carácter personal en la justicia penal (pp. 49–158). J. M. Bosch. <https://www.jstor.org/stable/j.ctv14t46p2.6>

Constitución de la República del Ecuador. (2008). Registro Oficial 449, 20 de octubre de 2008.

ISMS Forum. (2025). El libro blanco del DPO (2.^a ed.).

Ley Orgánica de Protección de Datos Personales. (2021). Quinto Suplemento del Registro Oficial 459, 26 de mayo de 2021 (reformada el 22 de mayo de 2026).

Morales, S. (2019). Derechos digitales y regulación de Internet: Aspectos claves de la apropiación de tecnologías digitales. En A. L. Rivoir & M. J. Morales (Eds.), *Tecnologías digitales: Miradas críticas de la apropiación en América Latina* (pp. 35–50). CLACSO. <https://www.jstor.org/stable/j.ctvt6rmh6.5>

Reglamento General de la Ley Orgánica de Protección de Datos Personales, Decreto Ejecutivo 904. (2023). Tercer Suplemento del Registro Oficial 435, 13 de noviembre de 2023.

Trujillo Cabrera, C., & Lorenzo Cabrera, S. (2021). La protección de datos en la investigación jurídica. En M. A. Calzadilla Medina, M. T. Manescau Martín, & J. J. Rodríguez Bravo de Laguna (Eds.), *Iniciación a la investigación jurídica* (pp. 93–100). Dykinson. <https://www.jstor.org/stable/j.ctv1ks0gn4.12>

UNESCO. (2026). Directrices para el uso de sistemas de IA en cortes y tribunales. <https://www.jstor.org/stable/resrep79108.7>