



UNIVERSIDAD ESTATAL DE MILAGRO

REPÚBLICA DEL ECUADOR

UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

FACULTAD DE POSGRADOS

ARTÍCULOS ACADÉMICOS CIENTÍFICOS DE ALTO NIVEL
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAESTRÍA EN DERECHOS HUMANOS CON MENCIÓN EN SISTEMAS
INTERNACIONALES DE PROTECCIÓN

TEMA:

Memoria digital íntima y obligaciones estatales frente a plataformas privadas:
insuficiencias regulatorias y procesales constitucionales en América Latina

Autores:

Abg. Diego Andrés Delgado Prieto

Abg. Marcela Yulieth López Caicedo

Tutor:

Msc. José Alejandro Villalta León

Milagro, 2026

Resumen

Este artículo examina las obligaciones de Colombia y Ecuador frente a la protección de la memoria digital íntima en plataformas privadas, a la luz de los estándares del Sistema Universal e Interamericano de Derechos Humanos. Mediante un enfoque jurídico cualitativo, analítico y documental, con componente de derecho comparado que incorpora los ordenamientos de Brasil, Argentina, México y Chile, se determinó que los países estudiados carecen de mecanismos regulatorios específicos para supervisar la retención y eliminación de datos íntimos almacenados por plataformas globales. Se propone la figura del habeas data colectivo como mecanismo procesal constitucional adaptado a la dimensión transnacional de estas vulneraciones.

Palabras clave: memoria digital íntima, autodeterminación informativa, responsabilidad estatal, plataformas digitales, garantías procesales constitucionales.

Abstract

This article examines the obligations of Colombia and Ecuador regarding the protection of intimate digital memory on private platforms, in light of the Universal and Inter-American Human Rights Systems. Through a qualitative, analytical, and documentary legal approach, with a comparative law component incorporating Brazil, Argentina, Mexico, and Chile, the study found that the countries examined lack specific regulatory mechanisms to oversee the retention and deletion of intimate data stored by global platforms. The article proposes collective habeas data as a constitutional procedural mechanism adapted to the transnational dimension of these violations.

KEYWORDS: intimate digital memory, informational self-determination, state responsibility, digital platforms, constitutional procedural guarantees.

1. INTRODUCCIÓN

La transformación digital de las últimas dos décadas ha modificado de manera sustancial la forma en que las personas construyen, almacenan y comparten los registros de su vida cotidiana. Lo que antes quedaba confinado a diarios personales, álbumes fotográficos o correspondencia epistolar, hoy se deposita —con frecuencia de modo inadvertido— en servidores controlados por corporaciones tecnológicas cuya sede, jurisdicción y políticas internas escapan al alcance directo de los ordenamientos jurídicos nacionales. Fotografías familiares, conversaciones privadas, historiales de navegación, registros de geolocalización, datos biométricos y preferencias de consumo conforman un acervo que puede denominarse *memoria digital íntima*: el conjunto de datos, registros y contenidos de naturaleza personal y sensible que una persona genera, almacena o comparte en entornos digitales y que guardan relación directa con su identidad, su vida privada y su dignidad (Mayer-Schönberger, 2009; Solove, 2008). Esta noción se diferencia del concepto genérico de datos personales en la medida en que acentúa la dimensión biográfica, afectiva y existencial de la información, vinculándola al libre desarrollo de la personalidad y a la construcción autónoma de la propia narrativa vital (Rodotà, 2012).

El problema cobra relevancia particular si se considera que las grandes plataformas —Meta, Alphabet, ByteDance, Amazon, entre otras— operan bajo modelos de negocio cuya rentabilidad depende, en buena medida, de la recolección masiva y el procesamiento algorítmico de datos personales. La denominada economía de la vigilancia (Zuboff, 2015) ha convertido la información íntima de millones de personas en materia prima de una industria global sin que los titulares participen de manera informada en las decisiones que los afectan. El escándalo de Cambridge Analytica (Information Commissioner's Office, 2018) demostró cómo la explotación no consentida de datos personales puede alterar procesos democráticos y vulnerar derechos fundamentales a una escala difícilmente imaginable bajo los paradigmas clásicos del derecho constitucional.

Pese a estos desarrollos, la doctrina jurídica latinoamericana no ha abordado de manera sistemática la protección de la memoria digital íntima como categoría diferenciada de los datos personales comunes, ni ha examinado con suficiente profundidad las garantías procesales constitucionales disponibles —habeas data, acción de tutela, acción de protección— como instrumentos para enfrentar las vulneraciones provenientes de plataformas privadas transnacionales. Esta laguna resulta especialmente problemática en el ámbito del derecho

procesal constitucional, donde la eficacia de los derechos sustanciales depende de la existencia de mecanismos jurisdiccionales idóneos, accesibles y efectivos.

Frente a este vacío, la presente investigación formula la siguiente pregunta central: ¿resultan suficientes los marcos normativos, institucionales y procesales constitucionales vigentes en Colombia y Ecuador —y, por extensión, en América Latina— para garantizar la protección efectiva de la memoria digital íntima frente a la actuación de plataformas privadas, a la luz de los estándares del Sistema Universal e Interamericano de Derechos Humanos? La tesis que se sostiene es que tales marcos presentan deficiencias estructurales que exigen reformas legislativas específicas, fortalecimiento institucional de las autoridades de control y adaptación de las garantías procesales constitucionales a la dimensión transnacional de las amenazas digitales.

El artículo se organiza en siete apartados que siguen una progresión argumentativa deliberada. El marco teórico construye las herramientas conceptuales necesarias para el análisis, culminando con una propuesta de operacionalización de la memoria digital íntima y con el examen de las garantías procesales constitucionales como hilo conductor diferenciador. La metodología explicita las categorías de comparación y justifica la selección de seis países. El análisis de resultados aplica esas categorías de manera uniforme. La discusión confronta los hallazgos con los estándares internacionales y propone figuras procesales novedosas. La conclusión formula recomendaciones con proyección legislativa y traza líneas de investigación futura.

2. MARCO TEÓRICO

2.1. Privacidad y memoria digital íntima: delimitación conceptual

La privacidad ha sido objeto de múltiples aproximaciones doctrinales que reflejan la evolución de las amenazas a la esfera personal en cada época. Solove (2002) propuso una taxonomía funcional que identifica cuatro grandes grupos de actividades lesivas: la recolección, el procesamiento, la diseminación y la invasión de información personal. Cada una de esas categorías adquiere matices nuevos en el entorno digital, donde la capacidad técnica de almacenamiento y cruce de datos supera con creces la de cualquier medio analógico anterior. Nissenbaum (2004) complementó esta perspectiva al plantear que la privacidad no depende de un principio de secreto absoluto, sino de la adecuación del flujo informacional a las normas contextuales que gobiernan cada ámbito de la vida social. Una fotografía compartida en un grupo cerrado de mensajería, por ejemplo, satisface las normas informacionales de confianza

entre sus participantes; su difusión ulterior por parte de la plataforma para fines publicitarios quebranta esas normas, aun cuando no medie un acto de intrusión en sentido clásico.

Desde esta base, cabe construir la categoría de memoria digital íntima como noción específica dentro del universo más amplio de los datos personales. Mayer-Schönberger (2009) advirtió que la transición de una cultura del olvido natural a una cultura de la memoria digital permanente constituía uno de los retos más profundos para la libertad individual en el siglo XXI. Las plataformas no solo almacenan lo que el usuario deposita de manera consciente — publicaciones, fotografías, mensajes—, sino que generan capas adicionales de información inferida a partir de patrones de comportamiento, metadatos de conexión y algoritmos de perfilamiento que el titular desconoce en la mayoría de los casos. El resultado es un doble digital que puede ser más revelador que cualquier confesión verbal y cuya persistencia temporal excede la voluntad del individuo que lo originó.

Conviene precisar en qué se diferencia la memoria digital íntima de las categorías convencionales que maneja la dogmática jurídica de protección de datos. El concepto de dato personal, tal como lo define la Ley 1581 de 2012 en Colombia o el RGPD en Europa, alude a cualquier información que permita identificar o hacer identificable a una persona; su finalidad protectora gira en torno a la identidad y la identificabilidad, y el riesgo principal que enfrenta es la identificación no consentida. Los datos sensibles, por su parte, constituyen una subcategoría cualificada que abarca información sobre origen étnico, salud, vida sexual, creencias religiosas o datos biométricos; aquí el ordenamiento jurídico establece una protección reforzada porque el riesgo predominante es la discriminación. La memoria digital íntima, en cambio, no se reduce a un dato aislado ni a una categoría cualificada por su contenido: se trata de un conjunto biográfico acumulativo de registros que una persona genera, almacena y comparte a lo largo del tiempo en entornos digitales, y que guardan relación directa con la integridad de su relato vital, su dignidad y el libre desarrollo de su personalidad. Mientras el dato personal opera en el plano del presente y el dato sensible en el plano de la vulnerabilidad cualificada, la memoria digital íntima opera en el plano de la persistencia histórica, donde el riesgo cardinal no es la identificación ni la discriminación, sino la descontextualización, la instrumentalización comercial y la pérdida irreversible de control sobre la propia narrativa personal (Solove, 2008; Nissenbaum, 2004; Mayer-Schönberger, 2009; Rodotà, 2012). De allí que la protección exigible deba ser máxima, orientada a preservar la integridad del acervo biográfico digital como condición para el ejercicio pleno de la autonomía individual.

La dimensión jurídica de esta problemática se inscribe en la tradición constitucional que reconoce la intimidad como derecho fundamental autónomo. En el ámbito europeo, la

sentencia del Tribunal de Justicia de la Unión Europea en el caso Google Spain c. AEPD y Costeja González (C-131/12, 2014) consagró el derecho al olvido digital al reconocer que el interesado puede exigir la desindexación de resultados inadecuados o excesivos. En el contexto latinoamericano, la Corte Constitucional de Colombia, mediante la sentencia T-277 de 2015, reconoció que la permanencia indefinida de cierta información en la red puede lesionar la dignidad y la autodeterminación de la persona afectada (Aristizábal Correa, 2019).

2.2. Dignidad humana y autodeterminación informativa

La dignidad humana opera como principio fundante del ordenamiento constitucional y como criterio hermenéutico para la interpretación de los derechos fundamentales en contextos de incertidumbre tecnológica. Pérez Luño (2005) ha sostenido que la dignidad impone al Estado la obligación de crear condiciones materiales e institucionales para que cada persona pueda desarrollar libremente su personalidad. En el entorno digital, esa obligación se traduce en garantizar que el tratamiento automatizado de datos no reduzca al individuo a la condición de mero objeto de perfilamiento algorítmico. Han (2017) ha profundizado en esta línea al argumentar que las tecnologías digitales instauran una forma de dominación psicopolítica en la que los individuos se autoexponen voluntariamente, lo cual no legitima la explotación de sus datos sino que, por el contrario, refuerza el deber estatal de proteger al ciudadano frente a una exposición cuyas consecuencias no puede anticipar cabalmente.

La noción de autodeterminación informativa (*informationelle Selbstbestimmung*) fue acuñada por el Tribunal Constitucional Federal de Alemania en la sentencia del censo de 1983 (BVerfGE 65, 1), donde se declaró que el derecho general de la personalidad comprende la facultad del individuo de decidir cuándo y dentro de qué límites se revelan datos relativos a su vida personal. Lucas Murillo de la Cueva (2007) señaló que esta construcción dogmática desplazó el eje de protección desde la esfera pasiva de la intimidad hacia la dimensión activa del control sobre los propios datos. Contreras Vásquez (2020) ha documentado cómo este principio fue recepcionado en las constituciones latinoamericanas, aunque con grados variables de desarrollo legislativo y jurisprudencial.

En América Latina, la autodeterminación informativa encontró acogida a través del *habeas data*, presente en las constituciones de Colombia (art. 15), Ecuador (art. 92), Brasil (art. 5, LXXII, Constitución de 1988) y Argentina (art. 43, Constitución de 1994). Puccinelli (2004) documentó la diversificación de esta garantía en múltiples variantes —*habeas data* propio, impropio, informativo, aditivo, rectificador, cancelatorio, reservador—. Con todo, como advierte Remolina Angarita (2013), la existencia formal del *habeas data* no equivale a una protección efectiva, pues su alcance práctico depende de la robustez del marco regulatorio

secundario, de la capacidad institucional de las autoridades de control y de la cultura jurídica de los operadores de justicia.

En el caso colombiano, la evolución normativa reciente ha reforzado parcialmente estas garantías. La Ley 2157 de 2021 modificó la Ley 1266 de 2008 con el propósito de fortalecer el derecho al habeas data financiero, reducir los plazos de permanencia de la información negativa y establecer mecanismos más ágiles de actualización y eliminación de datos crediticios. Si bien esta reforma se circunscribe al ámbito financiero, su aprobación refleja una tendencia legislativa favorable al fortalecimiento del control individual sobre los propios datos. En el terreno académico, Guerrero (2025) ha documentado cómo la doctrina constitucional colombiana sobre autodeterminación informativa podría extenderse a campos emergentes como las neurotecnologías, evidenciando que el marco conceptual desarrollado por la Corte Constitucional desde la sentencia T-414 de 1992 posee una capacidad de irradiación que trasciende los supuestos de hecho originalmente contemplados. Esta constatación resulta pertinente para la presente investigación, en la medida en que sugiere que las categorías constitucionales colombianas sobre habeas data y autodeterminación informativa disponen de la flexibilidad dogmática necesaria para acoger la noción de memoria digital íntima, aunque ello requiera un desarrollo legislativo complementario que el ordenamiento vigente aún no ha producido.

2.3. Responsabilidad estatal y efecto horizontal de los derechos fundamentales

Los Principios Rectores sobre las Empresas y los Derechos Humanos (Ruggie, 2011), adoptados por el Consejo de Derechos Humanos de las Naciones Unidas, establecieron un marco tripartito: el deber del Estado de proteger contra violaciones cometidas por terceros, la responsabilidad de las empresas de respetar los derechos humanos y la necesidad de garantizar mecanismos de reparación efectivos. Este marco resulta directamente aplicable a las plataformas digitales, que ejercen funciones que afectan derechos fundamentales de millones de personas sin estar sujetas a los controles democráticos que rigen la actividad del poder público.

La doctrina del efecto horizontal de los derechos fundamentales —*Drittwirkung der Grundrechte*— proporciona soporte dogmático para exigir que los derechos constitucionales operen también en relaciones entre particulares. Klonick (2018) describió a las grandes plataformas como nuevos gobernantes que ejercen un poder normativo cuasi soberano sobre la privacidad de sus usuarios. Balkin (2016) propuso la figura del fiduciario de información, según la cual las plataformas que recaban datos asumen obligaciones análogas a las de un profesional que maneja información confidencial. Cohen (2019), sin embargo, ha cuestionado

la suficiencia de la categoría fiduciaria, argumentando que las asimetrías estructurales del capitalismo informacional desbordan los remedios contractuales y exigen intervención regulatoria de naturaleza pública. Esta tensión entre enfoques fiduciarios y regulatorios constituye uno de los debates más fecundos de la doctrina contemporánea sobre gobernanza digital.

En el Sistema Interamericano, la Corte IDH ha reconocido que el deber de garantía previsto en el artículo 1.1 de la Convención Americana comprende la obligación estatal de prevenir, investigar, sancionar y reparar violaciones cometidas por particulares. En el caso *Escher y otros vs. Brasil* (2009), la Corte estableció que la interceptación de comunicaciones privadas por agentes no estatales genera responsabilidad internacional del Estado cuando este ha omitido adoptar medidas legislativas y administrativas de protección. En *Tristán Donoso vs. Panamá* (2009), *Fontevecchia y D'Amico vs. Argentina* (2011) e *I.V. vs. Bolivia* (2016), la Corte construyó una doctrina progresiva sobre vida privada que reconoce la protección de la información personal y la autonomía del individuo sobre su esfera íntima.

En la esfera colombiana, Rojas (2020) ha analizado la evolución del derecho de protección de datos personales en el país respecto de estándares internacionales, concluyendo que si bien Colombia cuenta con un aparato constitucional y legal relativamente sólido, persisten deficiencias en la supervisión efectiva de los responsables del tratamiento, especialmente cuando se trata de actores transnacionales que operan plataformas digitales de alcance global. Del mismo modo, la Ley 2300 de 2023, que estableció medidas para proteger el derecho a la intimidad de los consumidores frente a contactos comerciales no deseados por medios electrónicos, evidencia una preocupación legislativa creciente por la dimensión digital de la vida privada, aunque su alcance se limita al marketing y no aborda la problemática integral de la memoria digital íntima. Estos desarrollos normativos, sumados a la Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio sobre inteligencia artificial y tratamiento de datos, confirman que el debate regulatorio colombiano avanza en la dirección correcta pero de manera fragmentaria e insuficiente frente a la magnitud de los desafíos que plantean las plataformas globales.

2.4. Marco internacional de protección: Sistema Universal, Interamericano y Europeo

El derecho a la privacidad goza de reconocimiento en los principales instrumentos internacionales: el artículo 12 de la Declaración Universal, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 11 de la Convención Americana y el artículo 8 del Convenio Europeo. El Consejo de Derechos Humanos de las Naciones Unidas ha aprobado sucesivas resoluciones sobre el derecho a la privacidad en la era digital —28/16

(2015), 42/15 (2019) y 48/4 (2021)— que afirman que los mismos derechos que asisten a las personas fuera de Internet deben protegerse en el entorno digital. Los informes del Alto Comisionado (A/HRC/39/29, 2018; A/HRC/48/31, 2021) abordan la vigilancia masiva, el perfilamiento algorítmico y la responsabilidad de empresas tecnológicas. La Relatora Especial sobre privacidad, Ana Brian Nougères, formuló recomendaciones sobre los principios de finalidad, minimización y eliminación de datos (A/HRC/52/37, 2023).

En el ámbito europeo, el RGPD (Reglamento 2016/679) constituye el referente normativo más completo. Su alcance extraterritorial ha generado lo que Bradford (2020) denomina el efecto Bruselas: la capacidad de la regulación europea para moldear prácticas globales de empresas tecnológicas. La Ley de Servicios Digitales (DSA, Reglamento 2022/2065) y la Ley de Mercados Digitales (DMA, Reglamento 2022/1925) complementan el RGPD con obligaciones de transparencia y auditoría algorítmica para plataformas de gran escala. El Convenio 108+ del Consejo de Europa (2018) amplía la protección con principios de tratamiento lícito, seguridad y transferencia transfronteriza. Kuner, Bygrave y Docksey (2020) han analizado la complejidad de este entramado regulatorio y su potencial de influencia global.

En el espacio interamericano, la Relatoría Especial para la Libertad de Expresión de la CIDH publicó en 2017 estándares para una Internet libre, abierta e incluyente (OEA/Ser.L/V/II CIDH/RELE/INF.17/17), abordando la relación entre privacidad y empresas intermediarias. La Declaración Conjunta sobre Libertad de Expresión e Internet (2011) de los relatores especiales de la ONU, OSCE, OEA y CADHP subrayó la obligación de los Estados de proteger la privacidad en línea. La Red Iberoamericana de Protección de Datos adoptó en 2017 estándares regionales que buscan armonizar las legislaciones nacionales con los principios internacionales.

2.5. Plataformas digitales: entre autorregulación y regulación estatal

Gillespie (2018) documentó cómo las plataformas construyen sistemas de moderación que funcionan como ordenamientos normativos autónomos. Suzor (2019) profundizó al señalar que la gobernanza privada de Internet genera una situación de juridicidad sin ley, en la que los derechos de los usuarios dependen de decisiones corporativas opacas. Frente a esta realidad, la doctrina del constitucionalismo digital (Celeste, 2019; De Gregorio, 2022) propone la extensión de los principios constitucionales al espacio digital, exigiendo estándares mínimos de debido proceso, transparencia y no discriminación. Los Principios de Santa Clara (Electronic Frontier Foundation et al., 2021) representan un esfuerzo de la sociedad civil por establecer parámetros auditables, aunque su naturaleza voluntaria limita su eficacia.

La insuficiencia de la autorregulación ha quedado acreditada por episodios concretos que trascienden el caso Cambridge Analytica. Investigaciones periodísticas y regulatorias han documentado que plataformas como Meta conservan copias de datos personales —incluyendo fotografías, mensajes y registros de actividad— durante períodos que exceden con creces los plazos declarados en sus políticas de privacidad, incluso después de que los usuarios solicitan la eliminación de sus cuentas. La Comisión de Protección de Datos de Irlanda sancionó a Meta con multas superiores a los 1.200 millones de euros entre 2021 y 2023 por transferencias ilegales de datos de usuarios europeos a Estados Unidos, lo que demuestra que los incentivos de mercado resultan insuficientes para disuadir prácticas lesivas cuando la explotación de datos genera beneficios económicos que superan con creces el costo de las sanciones. Pasquale (2020) ha argumentado que la regulación tecnológica no puede dejarse en manos de quienes diseñan y comercializan las tecnologías, del mismo modo en que la regulación farmacéutica no se delega en los laboratorios.

2.6. Garantías procesales constitucionales como mecanismos de protección digital

Desde la óptica del derecho procesal constitucional, la efectividad de los derechos sustanciales depende de la existencia de vías jurisdiccionales idóneas para su defensa. En materia de protección de datos, el habeas data se ha consolidado como la garantía procesal específica en América Latina, aunque su configuración varía significativamente entre los ordenamientos estudiados. En Colombia, la acción de tutela (art. 86 de la Constitución de 1991) opera como mecanismo subsidiario cuando no existe otro medio de defensa judicial, y la Corte Constitucional la ha empleado extensivamente para resolver controversias sobre datos personales en entornos digitales, como se evidencia en la línea jurisprudencial que va de la sentencia T-414 de 1992 a la SU-420 de 2019. En Ecuador, la acción de habeas data está consagrada en el artículo 92 de la Constitución de 2008 como garantía jurisdiccional autónoma, regulada por la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009).

Las diferencias procesales entre ambos mecanismos son relevantes para el análisis. La tutela colombiana debe resolverse en diez días hábiles (art. 86 de la Constitución), admite la revisión eventual de la Corte Constitucional y puede dirigirse contra particulares que presten servicios públicos o cuya conducta afecte gravemente el interés colectivo. El habeas data ecuatoriano, en cambio, sigue el procedimiento de las garantías jurisdiccionales ordinarias establecido en la LOGJCC (arts. 47–49), con un plazo de resolución de ocho días tras la audiencia, y procede específicamente para acceder, actualizar, eliminar o anular datos que consten en registros públicos o privados. Pese a que ambos mecanismos han demostrado utilidad frente a responsables nacionales del tratamiento, ninguno fue diseñado para enfrentar

los desafíos que plantean las plataformas transnacionales: la determinación de la jurisdicción competente cuando el responsable carece de domicilio en el país, la ejecución de sentencias que ordenan la eliminación de datos almacenados en servidores extranjeros, y la eficacia de medidas cautelares frente a corporaciones que operan bajo ordenamientos jurídicos que no reconocen las decisiones judiciales de terceros Estados.

La experiencia brasileña con el Marco Civil de Internet (Ley 12.965 de 2014) ofrece un precedente relevante al establecer que las empresas de Internet quedan sometidas a la jurisdicción brasileña cuando ofrezcan servicios al público en ese país, con independencia de su lugar de constitución. Este modelo de jurisdicción basada en la prestación del servicio podría inspirar reformas procesales en Colombia y Ecuador orientadas a superar el obstáculo de la extraterritorialidad.

El recorrido conceptual y normativo desarrollado en este marco teórico conduce a una hipótesis que vertebra el análisis posterior: los ordenamientos jurídicos de Colombia y Ecuador —y, por extensión, los de la región latinoamericana— adolecen de una insuficiencia estructural para proteger la memoria digital íntima frente a las plataformas privadas transnacionales, tanto en el plano sustantivo (ausencia de regulación diferenciada sobre retención, eliminación y portabilidad de datos biográficos acumulativos) como en el plano procesal constitucional (inadecuación de las garantías jurisdiccionales vigentes para enfrentar responsables extraterritoriales). Esta insuficiencia no obedece a una mera laguna normativa puntual, sino a un desfase profundo entre las categorías jurídicas heredadas del constitucionalismo analógico y la arquitectura de poder que caracteriza al capitalismo informacional contemporáneo. Verificar o refutar esta hipótesis exige el examen comparado que se emprende en los apartados siguientes, apoyado en la metodología y las categorías de análisis que se describen a continuación.

3. METODOLOGÍA

El presente artículo se sustenta en una investigación jurídica cualitativa de carácter analítico, doctrinario y documental. La adopción de este enfoque responde a la naturaleza misma del objeto de estudio: la memoria digital íntima y las obligaciones estatales que derivan de su protección no constituyen fenómenos susceptibles de medición cuantitativa, sino realidades jurídicas complejas que demandan un ejercicio de interpretación profunda de normas, sentencias, instrumentos internacionales y construcciones doctrinales. Hernández Sampieri y Mendoza Torres (2018) sostienen que la investigación cualitativa permite comprender fenómenos complejos desde la interpretación profunda de documentos y discursos,

lo cual resulta particularmente pertinente cuando el investigador busca determinar el sentido y alcance de categorías jurídicas que aún no han sido plenamente formalizadas por el ordenamiento positivo. En esa línea, la investigación no se propuso recolectar datos numéricos ni aplicar encuestas o instrumentos estadísticos, sino estudiar normas internacionales y constitucionales, analizar jurisprudencia de tribunales nacionales e internacionales, revisar doctrina especializada y contrastar las obligaciones estatales frente al fenómeno digital contemporáneo.

3.1. Tipo de investigación

La investigación que fundamenta este artículo es de tipo descriptivo, analítico y crítico, tres dimensiones que operan de manera complementaria a lo largo del desarrollo argumentativo. En su dimensión descriptiva, el estudio identifica y sistematiza el marco normativo y doctrinal existente en materia de protección de datos personales, privacidad digital y garantías procesales constitucionales en Colombia, Ecuador y otros países de referencia, así como en los instrumentos del Sistema Universal e Interamericano de Derechos Humanos. Esta labor descriptiva no se agota en la enumeración de normas y sentencias, sino que organiza el material jurídico de manera que permita visualizar las convergencias, divergencias y vacíos entre los distintos ordenamientos.

En su dimensión analítica, la investigación va más allá de la descripción para examinar el alcance real de las obligaciones estatales frente a la protección de la memoria digital íntima. Ello implica descomponer las normas en sus elementos constitutivos, identificar las relaciones de coherencia o contradicción entre el derecho interno y los estándares internacionales, y evaluar si los mecanismos procesales disponibles resultan idóneos para enfrentar las amenazas que provienen de las plataformas tecnológicas transnacionales. Tantaleán Odar (2016) ha señalado que la investigación jurídica analítica se distingue de la meramente descriptiva en la medida en que no se limita a exponer el estado de la cuestión, sino que interroga críticamente las razones, los fundamentos y las consecuencias de las soluciones normativas vigentes.

Finalmente, en su dimensión crítica, el artículo formula juicios valorativos sustentados académicamente sobre la suficiencia o insuficiencia de los marcos regulatorios estudiados, proponiendo categorías conceptuales nuevas —como la memoria digital íntima— y mecanismos procesales innovadores —como el habeas data colectivo— que puedan contribuir al fortalecimiento de la protección de derechos humanos en entornos digitales. Esta dimensión crítica es la que distingue al artículo de un ejercicio puramente descriptivo o compilatorio y la que le confiere su carácter propositivo.

3.2. Métodos de investigación

Para el desarrollo del análisis se emplearon cuatro métodos de investigación jurídica, cada uno de los cuales cumple una función específica dentro de la arquitectura argumentativa del artículo.

El método exegético-jurídico se aplicó para el estudio directo de las normas que conforman el corpus regulatorio relevante. Mediante este método se analizaron, entre otros instrumentos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 11 de la Convención Americana sobre Derechos Humanos, las resoluciones 28/16, 42/15 y 48/4 del Consejo de Derechos Humanos de las Naciones Unidas, los artículos 15 y 86 de la Constitución Política de Colombia, la Ley Estatutaria 1581 de 2012, la Ley 2157 de 2021, los artículos 66.19 y 92 de la Constitución del Ecuador y la Ley Orgánica de Protección de Datos Personales de 2021. La exégesis permitió identificar el contenido prescriptivo de cada disposición, sus destinatarios, sus condiciones de aplicación y sus limitaciones frente al fenómeno de las plataformas digitales globales.

El método analítico-sistemático complementó la exégesis al poner en relación las normas analizadas entre sí, buscando identificar las conexiones funcionales entre el derecho internacional de los derechos humanos, el derecho constitucional interno y la legislación secundaria de protección de datos. Este método resultó indispensable para determinar si el conjunto normativo de cada país estudiado configura un sistema coherente de protección frente a la actuación de plataformas privadas, o si, por el contrario, presenta fisuras, contradicciones o vacíos que debilitan la eficacia de las garantías formalmente reconocidas. Villabella Armengol (2020) ha destacado que el análisis sistemático constituye una herramienta imprescindible en la investigación jurídica contemporánea, donde la fragmentación normativa y la pluralidad de fuentes exigen un esfuerzo de integración que trasciende la lectura aislada de cada disposición.

El método dogmático-jurídico se utilizó para interpretar las categorías conceptuales que articulan el marco teórico del artículo: privacidad, dignidad humana, autodeterminación informativa, efecto horizontal de los derechos fundamentales, memoria digital íntima y habeas data. Mediante este método se reconstruyó el sentido dogmático de cada categoría a partir de la doctrina autorizada, se identificaron las tensiones entre distintas aproximaciones teóricas — como la tensión entre el enfoque fiduciario de Balkin (2016) y el enfoque regulatorio de Cohen (2019)— y se propuso una articulación conceptual propia que permite situar la memoria digital íntima como una categoría diferenciada dentro del sistema de derechos fundamentales.

El método jurisprudencial se desplegó para el examen de las decisiones judiciales que han dado contenido y alcance a los derechos de protección de datos, intimidad y habeas data en los países estudiados. Se analizaron sentencias de la Corte Constitucional de Colombia (desde la T-414 de 1992 hasta la SU-420 de 2019), de la Corte Constitucional del Ecuador (sentencias No. 55-14-JD/20 y 2064-14-EP/21), del Supremo Tribunal Federal de Brasil (ADI 6.387/DF de 2020), de la Corte Suprema de Justicia de la Nación Argentina (caso Rodríguez c/ Google, 2014), del Tribunal de Justicia de la Unión Europea (caso Google Spain c. AEPD y Costeja González, C-131/12, 2014) y de la Corte Interamericana de Derechos Humanos (casos Tristán Donoso vs. Panamá, Escher y otros vs. Brasil, Fontevecchia y D'Amico vs. Argentina e I.V. vs. Bolivia). El análisis jurisprudencial no se limitó a la descripción de las decisiones, sino que identificó las líneas argumentativas, los estándares de protección construidos por cada tribunal y las insuficiencias detectables en su aplicación al ámbito de las plataformas digitales.

3.3. Técnicas de investigación

Las técnicas de investigación empleadas fueron cuatro: revisión bibliográfica especializada, análisis documental, análisis jurisprudencial comparado e interpretación de instrumentos internacionales de derechos humanos. La revisión bibliográfica especializada comprendió la consulta de artículos publicados en revistas indexadas (SciELO, Dialnet, Redalyc, SSRN), libros de editoriales académicas reconocidas (Oxford University Press, Cambridge University Press, Harvard University Press, Tirant lo Blanch, Laterza) e informes de organismos internacionales y organizaciones especializadas en derechos digitales. Se priorizaron publicaciones del período 2015-2025, sin excluir obras seminales anteriores que resultan indispensables para la comprensión de las categorías fundamentales.

El análisis documental permitió extraer, clasificar y sistematizar la información contenida en las fuentes normativas, doctrinales y jurisprudenciales, organizándola en torno a las categorías de análisis definidas para la comparación. El análisis jurisprudencial comparado posibilitó contrastar los estándares de protección construidos por los tribunales constitucionales de los seis países estudiados, identificando convergencias y divergencias en el tratamiento del derecho al olvido, la autodeterminación informativa y la responsabilidad de plataformas digitales. La interpretación de instrumentos internacionales de derechos humanos se realizó conforme a los principios de interpretación establecidos en la Convención de Viena sobre el Derecho de los Tratados (1969), particularmente el principio de buena fe, el sentido corriente de los términos y el objeto y fin del tratado.

3.4. Unidad de análisis: corpus documental

El corpus documental que sustenta la investigación está conformado por cinco categorías de fuentes. En primer lugar, tratados internacionales de derechos humanos vinculantes para los Estados estudiados, particularmente el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos. En segundo lugar, resoluciones e informes de órganos del Sistema Universal, entre los que se destacan las resoluciones del Consejo de Derechos Humanos sobre privacidad en la era digital, los informes del Alto Comisionado (A/HRC/39/29 y A/HRC/48/31) y los informes de la Relatora Especial sobre el derecho a la privacidad. En tercer lugar, los Principios Rectores sobre las Empresas y los Derechos Humanos adoptados en 2011. En cuarto lugar, normas constitucionales y legislación secundaria de protección de datos de Colombia (Constitución de 1991, Ley 1266 de 2008, Ley 1581 de 2012, Ley 2157 de 2021, Ley 2300 de 2023), Ecuador (Constitución de 2008, LOPDP de 2021), Brasil (Constitución de 1988, Marco Civil de Internet de 2014, LGPD de 2018), Argentina (Constitución de 1994, Ley 25.326 de 2000), Chile (Ley 21.719 de 2024) y México (LFPDPPP de 2010, LGPDPPSO de 2017), así como el RGPD europeo, la Ley de Servicios Digitales y la Ley de Mercados Digitales. En quinto lugar, sentencias de los tribunales constitucionales e internacionales mencionados en el apartado anterior, junto con la doctrina especializada que conforma la base bibliográfica del artículo.

La selección de los seis países responde a criterios de variación tipológica: Colombia y Ecuador como casos centrales por su pertinencia directa para la investigación; Brasil, por ser el único país de la región que ha reconocido jurisprudencialmente la protección de datos como derecho fundamental autónomo; Argentina, por su carácter pionero y su precedente emblemático sobre responsabilidad de motores de búsqueda; Chile, por su legislación de nueva generación; y México, por ofrecer un modelo dual público-privado que contrasta con los demás ordenamientos. Se excluyen países con desarrollos menos consolidados cuya incorporación habría ampliado el estudio sin aportar variaciones tipológicas sustanciales.

El estudio presenta limitaciones inherentes a su naturaleza documental: no incorpora trabajo de campo ni entrevistas con operadores de justicia, y la escasa disponibilidad de datos cuantitativos sobre la gestión de las autoridades de protección de datos en la región impide complementar el análisis normativo con una evaluación empírica de la eficacia institucional. Estas limitaciones, lejos de invalidar los hallazgos, delimitan el alcance de las conclusiones y abren espacio para investigaciones futuras de carácter empírico.

4. ANÁLISIS DE RESULTADOS

El análisis del corpus normativo, jurisprudencial y doctrinal descrito en la metodología permitió identificar seis hallazgos jurídicos principales que se presentan a continuación. Cada hallazgo se sustenta en las fuentes examinadas y se interpreta jurídicamente a la luz de la hipótesis formulada en el marco teórico. Los apartados 4.1 a 4.4 exponen el material comparado que respalda estos hallazgos, mientras que la síntesis final los consolida de manera diferenciada respecto de la discusión que se desarrolla en el apartado siguiente.

4.1. Colombia: avances jurisprudenciales y déficits regulatorios

Colombia dispone de uno de los marcos más desarrollados de la región. La Constitución de 1991 consagra en su artículo 15 el derecho a la intimidad, al buen nombre y a conocer, actualizar y rectificar la información recogida en bancos de datos. La Ley 1266 de 2008 reguló el habeas data financiero, mientras que la Ley Estatutaria 1581 de 2012, reglamentada por el Decreto 1377 de 2013, estableció el régimen general de protección de datos. La Superintendencia de Industria y Comercio (SIC) ejerce como autoridad de control con facultades de inspección, vigilancia y sanción, habiendo impuesto entre 2013 y 2024 más de 700 sanciones por infracciones al régimen de protección de datos, aunque la mayoría de ellas dirigidas a responsables nacionales y no a plataformas tecnológicas globales.

La jurisprudencia de la Corte Constitucional ha sido prolífica. Desde la sentencia T-414 de 1992, que sentó las bases del habeas data como derecho autónomo, la Corte ha construido una línea sostenida: sentencia T-729 de 2002 (principios de libertad, necesidad y circulación restringida), sentencia C-748 de 2011 (constitucionalidad de la Ley 1581), sentencia SU-458 de 2012 (olvido financiero), sentencia T-020 de 2014 (tratamiento estructurado de datos por motores de búsqueda), sentencia T-277 de 2015 (derecho al olvido digital frente a medios en línea) y sentencia SU-420 de 2019 (unificación sobre derecho al olvido como manifestación del habeas data). Pese a ello, como señalan Aristizábal Correa (2019) y Upegui Mejía (2017), la ausencia de regulación específica sobre plataformas tecnológicas globales genera zonas grises que la jurisprudencia no puede llenar por sí sola. La Ley 1581 no contempla mecanismos de eliminación efectiva de datos almacenados en servidores ubicados fuera de la jurisdicción colombiana, ni el derecho a la portabilidad de datos. Remolina Angarita (2010) ha advertido que Colombia enfrenta dificultades para alcanzar un nivel de protección equiparable al estándar europeo, en razón de limitaciones institucionales de la SIC y la insuficiente cooperación internacional en materia de transferencias transfronterizas.

4.2. Ecuador: la LOPDP y sus desafíos de implementación

Ecuador incorporó la protección de datos en el artículo 66, numeral 19, de la Constitución de 2008 y consagró el habeas data en el artículo 92. Con todo, durante más de una década careció de legislación secundaria integral. La Ley Orgánica de Protección de Datos Personales (LOPDP), aprobada en mayo de 2021, se inspiró en el RGPD europeo; su reglamento general se expidió en diciembre de 2023. La LOPDP establece principios de tratamiento lícito, finalidad, proporcionalidad y minimización, y reconoce derechos de acceso, rectificación, cancelación, oposición y portabilidad. Rosas-Lanas y Pila-Cárdenas (2023) destacaron que esta ley representa un avance significativo, si bien la Superintendencia de Protección de Datos Personales no alcanzó plena operatividad institucional hasta 2024, cuando comenzó a tramitar las primeras denuncias ciudadanas por tratamiento indebido de datos. La Corte Constitucional del Ecuador ha contribuido mediante sentencias como la No. 55-14-JD/20 (habeas data frente a entidades financieras) y la No. 2064-14-EP/21 (protección de datos sensibles de salud), pero aún no ha abordado directamente la problemática de plataformas digitales globales (Naranjo Godoy, 2017; Enríquez Álvarez, 2017).

4.3. Brasil: reconocimiento del derecho fundamental y la LGPD

Brasil ofrece un caso particularmente instructivo. El Marco Civil de Internet (Ley 12.965 de 2014) estableció principios de neutralidad y protección de datos, sometiendo a las empresas de Internet a la jurisdicción brasileña cuando ofrezcan servicios en el país. La Lei Geral de Proteção de Dados Pessoais (LGPD, Ley 13.709 de 2018) configuró un régimen integral inspirado en el RGPD, con una autoridad nacional independiente (ANPD) dotada de facultades normativas y sancionadoras. La ANPD publicó entre 2021 y 2024 más de treinta resoluciones regulatorias y comenzó a ejercer su potestad sancionatoria efectiva desde 2023. El Supremo Tribunal Federal, en la medida cautelar de la ADI 6.387/DF (2020), reconoció la protección de datos personales como derecho fundamental autónomo, anticipando su incorporación formal mediante la Enmienda Constitucional 115 de 2022. Doneda (2011) y Mendes y Fonseca (2020) han destacado que la experiencia brasileña demuestra la importancia de combinar un marco legislativo robusto con una autoridad independiente y una jurisprudencia constitucional activa. La cláusula de jurisdicción del Marco Civil constituye un modelo relevante para la regulación de plataformas transnacionales en la región.

4.4. Argentina, México y Chile: variaciones tipológicas

Argentina fue pionera al sancionar la Ley 25.326 de Protección de Datos Personales en el año 2000, obteniendo la declaración de adecuación europea. La Corte Suprema, en Rodríguez, María Belén c/ Google Inc. (2014), abordó la responsabilidad de los motores de

búsqueda por vinculación de imágenes íntimas a contenidos lesivos del honor, estableciendo criterios de ponderación que anticiparon la discusión regional sobre derecho al olvido. La ley argentina, sin embargo, no ha sido actualizada para incorporar derechos de portabilidad, evaluaciones de impacto o notificación obligatoria de brechas de seguridad, y la Agencia de Acceso a la Información Pública (AAIP) carece de recursos para supervisar efectivamente a plataformas globales. México cuenta con un marco dual: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) para el sector privado y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017) para el sector público, aunque el Instituto Nacional de Transparencia (INAI) ha visto reducidas sus capacidades operativas en años recientes, lo que compromete la supervisión efectiva del tratamiento de datos por parte de plataformas tecnológicas.

Chile merece atención particular por haber promulgado en diciembre de 2024 la Ley 21.719, que moderniza integralmente el régimen de protección de datos, crea la Agencia de Protección de Datos Personales y establece mecanismos de transferencia internacional alineados con el RGPD. Esta legislación de nueva generación fue posible tras la reforma constitucional de 2018, que incorporó la protección de datos como derecho fundamental autónomo en el artículo 19 numeral 4 de la Constitución (Contreras Vásquez, 2020). La Ley 21.719 incluye una cláusula de alcance extraterritorial que somete a su régimen a todo responsable o encargado del tratamiento que, sin tener establecimiento en Chile, trate datos de personas que se encuentren en el territorio nacional, lo cual la posiciona como la segunda legislación de la región —junto con la LGPD brasileña— en abordar frontalmente el desafío de la extraterritorialidad.

La Tabla 3 sintetiza los hallazgos del análisis comparado aplicando las siete categorías de la matriz metodológica.

Tabla 3

Análisis comparado: protección de la memoria digital íntima en seis países latinoamericanos

Categoría	Colombia	Ecuador	Brasil	Argentina	Chile	México
Rango constitucional	Sí (art. 15)	Sí (art. 66.19)	Sí (EC 115/2022)	Sí (art. 43)	Sí (art. 19.4)	Sí (art. 16)
Ley específica	L. 1581/2012	LOPDP 2021	LGPD 2018	L. 25.326/2000	L. 21.719/2024	LFPDPPP 2010
Autoridad de control	SIC (operativa)	SPDP (desde 2024)	ANPD (operativa)	AAIP (operativa)	Agencia (en creación)	INAI (debilitado)
Garantía procesal	Tutela + habeas data	Habeas data constitucional	Habeas data + mandato	Amparo + habeas data	Habeas data (art. 19.4)	Amparo + juicio de nulidad

de segurança						
Olvido digital	Jurisprudencial (SU-420/19)	Legislativo (LOPDP art. 26)	Legislativo (LGPD art. 18)	Jurisprudencial (Rodríguez 2014)	Legislativo (L. 21.719)	Parcial (vía ARCO)
Alcance extraterritorial	No expreso	Limitado (LOPDP art. 3)	Sí (LGPD art. 3 + MCI)	No expreso	Sí (L. 21.719 art. 1)	Limitado
Jurispr. plataformas	T-277/15, SU- 420/19	Incipiente	STJ y ANPD activos	CSJN Rodríguez/14	No consolidada	INAI resoluciones

Nota. Elaboración propia con base en legislación y jurisprudencia nacional vigente al primer trimestre de 2026.

El examen comparado revela patrones compartidos: todos los países reconocen constitucionalmente alguna forma de protección de datos, pero difieren significativamente en densidad regulatoria, capacidad institucional de las autoridades de control, extensión de los derechos del titular y regulación de plataformas digitales. En conjunto, Brasil presenta el grado más avanzado de protección —por la combinación de rango constitucional autónomo, legislación integral operativa, autoridad independiente activa y cláusula jurisdiccional sobre plataformas—, seguido por Chile —cuya legislación de 2024 lo posiciona como referente emergente— y Colombia —cuya fortaleza reside en su jurisprudencia constitucional, aunque su legislación requiere actualización—. Ecuador, Argentina y México exhiben brechas más pronunciadas en distintas categorías: Ecuador, por la reciente operatividad de su autoridad de control; Argentina, por la desactualización de su ley; y México, por el debilitamiento institucional del INAI. Ninguno de los ordenamientos contempla la categoría de memoria digital íntima como bien jurídico autónomo, ni establece obligaciones diferenciadas de diligencia debida para las plataformas que almacenan datos vinculados a la esfera biográfica de las personas. Las garantías procesales constitucionales, si bien formalmente disponibles, no han sido adaptadas a los desafíos jurisdiccionales que plantea la actuación de plataformas transnacionales.

4.5. Consolidación de hallazgos

A partir del examen comparado precedente, se identifican los siguientes hallazgos jurídicos.

Hallazgo 1. El Sistema Universal de Derechos Humanos impone a los Estados obligaciones positivas de protección de la privacidad digital frente a actores privados, incluidas las plataformas tecnológicas. Las resoluciones 28/16 (2015), 42/15 (2019) y 48/4 (2021) del Consejo de Derechos Humanos, junto con los informes del Alto Comisionado (A/HRC/39/29, 2018; A/HRC/48/31, 2021) y los Principios Rectores sobre las Empresas y los Derechos

Humanos (Ruggie, 2011), configuran un marco normativo internacional que exige a los Estados adoptar medidas legislativas, administrativas y jurisdiccionales para prevenir, investigar y reparar las vulneraciones de la privacidad cometidas por terceros en entornos digitales. Este deber no es meramente programático: se trata de obligaciones jurídicas vinculantes que derivan del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y del artículo 11 de la Convención Americana sobre Derechos Humanos, tal como han sido interpretados por los órganos de supervisión competentes.

Hallazgo 2. La legislación colombiana protege datos personales mediante un régimen general (Ley 1581 de 2012) y una garantía constitucional de habeas data (art. 15 de la Constitución), pero no regula de forma expresa la memoria digital íntima como categoría diferenciada de protección reforzada. La Ley 1581 fue concebida para un ecosistema digital menos complejo que el actual y no contempla obligaciones específicas sobre eliminación efectiva de datos almacenados en servidores extranjeros, portabilidad real de datos biográficos acumulativos ni plazos máximos verificables para la supresión de información íntima. La Ley 2157 de 2021 fortaleció el habeas data financiero, y la Ley 2300 de 2023 abordó la intimidad del consumidor frente a contactos comerciales no deseados, pero ninguna de estas reformas cerró la brecha regulatoria en materia de memoria digital íntima frente a plataformas globales. Remolina Angarita (2010) ha señalado que Colombia enfrenta dificultades estructurales para alcanzar un nivel de protección equiparable al estándar europeo, particularmente en lo relativo a la supervisión de actores transnacionales.

Hallazgo 3. La jurisprudencia constitucional colombiana reconoce indirectamente el derecho al olvido y la autodeterminación informativa en entornos digitales, pero su eficacia se ve limitada por la ausencia de mecanismos de ejecución frente a plataformas extraterritoriales. La línea jurisprudencial que va de la sentencia T-414 de 1992 a la SU-420 de 2019 ha construido un aparato dogmático sofisticado sobre habeas data, principios de tratamiento de datos y derecho al olvido. La sentencia T-277 de 2015, en particular, reconoció que la permanencia indefinida de información personal en medios digitales puede lesionar la dignidad del titular (Aristizábal Correa, 2019). Pese a ello, estas decisiones operan dentro de los límites jurisdiccionales del Estado colombiano y carecen de instrumentos procesales para vincular a corporaciones cuya sede y servidores se encuentran en otras jurisdicciones. Guerrero (2025) ha documentado que la doctrina constitucional colombiana sobre autodeterminación informativa posee una capacidad de irradiación que trasciende los supuestos originalmente contemplados, pero advierte que su efectividad depende del desarrollo legislativo complementario.

Hallazgo 4. Existe una asimetría de poder entre plataformas digitales y ciudadanos que supera el simple consentimiento contractual y que los ordenamientos latinoamericanos no han abordado adecuadamente. Las plataformas tecnológicas no se limitan a almacenar los datos que el usuario deposita de manera consciente; generan capas adicionales de información inferida a partir de patrones de comportamiento, metadatos y algoritmos de perfilamiento que el titular desconoce (Mayer-Schönberger, 2009; Zuboff, 2015). Esta asimetría informacional y económica torna ilusorio el consentimiento como base exclusiva de legitimación del tratamiento de datos, lo cual ha llevado a la doctrina contemporánea a cuestionar la suficiencia de los enfoques fiduciarios (Balkin, 2016) y a proponer modelos de regulación pública obligatoria (Cohen, 2019). En los seis países estudiados, el consentimiento sigue siendo el eje central del régimen de protección de datos, sin que se hayan desarrollado mecanismos efectivos para compensar la desigualdad estructural entre las partes.

Hallazgo 5. Las garantías procesales constitucionales disponibles en la región —tutela, habeas data, amparo— no están adaptadas a la dimensión transnacional de las plataformas digitales. Como se documentó en los apartados 4.1 a 4.4, la tutela colombiana y el habeas data ecuatoriano fueron diseñados para enfrentar responsables del tratamiento localizables dentro de la jurisdicción nacional. La determinación de la jurisdicción competente cuando el responsable carece de domicilio en el país, la ejecución de sentencias que ordenan la eliminación de datos almacenados en servidores extranjeros y la eficacia de medidas cautelares frente a corporaciones que operan bajo otros ordenamientos jurídicos constituyen obstáculos procesales que la dogmática constitucional aún no ha resuelto de manera satisfactoria. Solo Brasil, mediante la cláusula jurisdiccional del Marco Civil de Internet (2014), y Chile, mediante la Ley 21.719 (2024), han adoptado mecanismos de alcance extraterritorial que permiten someter a plataformas extranjeras a la jurisdicción nacional cuando estas ofrecen servicios u obtienen datos de personas ubicadas en su territorio.

Hallazgo 6. El análisis comparado de seis países latinoamericanos revela que ningún ordenamiento contempla la categoría de memoria digital íntima como bien jurídico autónomo merecedor de protección diferenciada. Todos los países reconocen constitucionalmente alguna forma de protección de datos, pero difieren significativamente en densidad regulatoria, capacidad institucional de las autoridades de control y regulación de plataformas digitales. Brasil presenta el grado más avanzado de protección, seguido por Chile y Colombia, mientras que Ecuador, Argentina y México exhiben brechas más pronunciadas en distintas categorías, conforme se sintetiza en la Tabla 3. Esta constatación confirma la hipótesis formulada en el

marco teórico sobre la insuficiencia estructural de los marcos regulatorios latinoamericanos frente a la protección de la memoria digital íntima.

5. DISCUSIÓN

Los hallazgos presentados en el apartado anterior exigen un ejercicio de interpretación y confrontación crítica que permita determinar qué significan, qué implican y qué consecuencias generan para el derecho procesal constitucional y para la protección de los derechos humanos en entornos digitales. La discusión se organiza en torno a tres operaciones intelectuales diferenciadas: la comparación de los hallazgos con la doctrina y los estándares internacionales, la interpretación de las brechas detectadas y la argumentación de la posición investigativa propia.

5.1. Comparación de hallazgos con la doctrina y los estándares internacionales

Los hallazgos 1 y 2 confirman lo que Bradford (2023) ha descrito como una tensión entre imperios digitales regulatorios: mientras el RGPD europeo ha configurado un modelo de protección integral con alcance extraterritorial, auditoría algorítmica y sanciones disuasorias, los países latinoamericanos operan con legislaciones concebidas para un ecosistema digital menos complejo. La distancia entre las resoluciones del Consejo de Derechos Humanos —que exigen a los Estados regular a los actores privados cuyas actividades afectan derechos en el entorno digital— y la realidad normativa de Colombia y Ecuador evidencia un incumplimiento parcial de las obligaciones internacionales que estos Estados han asumido voluntariamente al ratificar el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana. Los hallazgos 3 y 4 coinciden con la crítica de Cohen (2019), para quien las asimetrías estructurales del capitalismo informacional desbordan los remedios contractuales y fiduciarios y exigen intervención regulatoria de naturaleza pública. La jurisprudencia constitucional colombiana —particularmente la sentencia SU-420 de 2019— ha avanzado en la construcción de estándares sobre derecho al olvido, pero su alcance se ve neutralizado por la imposibilidad práctica de vincular a plataformas extraterritoriales.

5.2. Interpretación de las brechas detectadas

Las brechas identificadas en los hallazgos 5 y 6 no obedecen a una mera laguna normativa puntual que pueda resolverse con ajustes técnicos menores. Se trata de una inadecuación profunda entre las categorías jurídicas heredadas del constitucionalismo analógico —diseñadas para regular relaciones de poder entre el Estado y los ciudadanos, o entre particulares dentro de una misma jurisdicción— y la arquitectura de poder que caracteriza al capitalismo informacional contemporáneo, donde corporaciones con sede en unas pocas jurisdicciones concentran la capacidad de almacenar, procesar y explotar los datos biográficos

de miles de millones de personas distribuidas en todos los países del mundo. Zuboff (2015) ha denominado a esta dinámica capitalismo de la vigilancia, y su lógica resulta estructuralmente incompatible con una protección robusta de la privacidad basada en el consentimiento individual. En términos prácticos, esto significa que un ciudadano colombiano o ecuatoriano que solicite la eliminación de sus datos íntimos almacenados por una plataforma con sede en Estados Unidos enfrenta obstáculos jurisdiccionales, procesales y de ejecución que tornan ilusoria la garantía constitucional del habeas data tal como está configurada actualmente. La insuficiencia no es accidental: refleja un desfase estructural entre la velocidad de la transformación tecnológica y la capacidad de respuesta de los sistemas jurídicos nacionales.

5.3. Argumentación de la posición investigativa

A la luz de los hallazgos y de su interpretación, sostengo que el Estado colombiano — y, en términos análogos, el ecuatoriano— incumple parcialmente sus obligaciones de garantía en materia de protección de la memoria digital íntima frente a plataformas privadas transnacionales. Este incumplimiento no se manifiesta en la ausencia total de regulación, sino en la insuficiencia de los mecanismos existentes para hacer frente a un fenómeno que desborda las categorías del derecho interno. Tres argumentos respaldan esta posición.

En primer lugar, la obligación de protección derivada del artículo 1.1 de la Convención Americana y del artículo 2 del Pacto Internacional comprende el deber de adoptar medidas legislativas y de otro carácter que sean necesarias para hacer efectivos los derechos reconocidos. La Corte Interamericana ha reiterado que este deber se extiende a las violaciones cometidas por particulares cuando el Estado ha omitido la diligencia debida (caso Escher y otros vs. Brasil, 2009). Frente a las plataformas digitales, la diligencia debida exige, como mínimo, la adopción de cláusulas jurisdiccionales de alcance extraterritorial, la creación de autoridades de control con capacidad técnica y financiera para supervisar a actores transnacionales, y la regulación de obligaciones específicas de eliminación efectiva y portabilidad de datos íntimos. Ninguno de estos elementos está plenamente desarrollado en el ordenamiento colombiano ni en el ecuatoriano.

En segundo lugar, las garantías procesales constitucionales vigentes resultan inadecuadas para abordar vulneraciones sistémicas de la memoria digital íntima. La tutela colombiana y el habeas data ecuatoriano fueron concebidos como instrumentos de protección individual frente a responsables localizables. La experiencia del litigio estructural desarrollado por la Corte Constitucional de Colombia en materia de desplazamiento forzado (sentencia T-025 de 2004) demuestra que el derecho procesal constitucional dispone de herramientas para abordar violaciones masivas y estructurales de derechos fundamentales, mediante la

declaratoria de estados de cosas inconstitucionales y la emisión de órdenes complejas dirigidas a múltiples actores. La adaptación de esta figura al ámbito de la protección de datos frente a plataformas —un habeas data colectivo o estructural— constituye una vía procesal que merece exploración legislativa y doctrinal.

En tercer lugar, la autorregulación empresarial no puede sustituir la regulación estatal en esta materia. Los episodios documentados en este artículo —las sanciones multimillonarias a Meta por transferencias ilegales de datos, la conservación indebida de datos de cuentas eliminadas, la opacidad algorítmica en el perfilamiento de usuarios— confirman que los incentivos de mercado resultan insuficientes para disuadir prácticas lesivas cuando la rentabilidad del modelo de negocio depende precisamente de la acumulación de datos íntimos. Pasquale (2020) ha argumentado que la regulación tecnológica no puede dejarse en manos de quienes diseñan y comercializan las tecnologías, del mismo modo en que la regulación farmacéutica no se delega en los laboratorios. La posición de quienes defienden la autorregulación —sosteniendo que las brechas de seguridad generan costos reputacionales que disciplinan a las empresas— desconoce que los costos de las vulneraciones de privacidad se externalizan predominantemente hacia los titulares de los datos, mientras que los beneficios de la explotación masiva se concentran en las corporaciones.

En definitiva, lo que este artículo detecta no es una deficiencia técnica menor, sino un problema de arquitectura jurídica que compromete la eficacia de los derechos fundamentales en el entorno donde transcurre, cada vez con mayor intensidad, la vida cotidiana de las personas. La respuesta a este problema no puede ser exclusivamente nacional: requiere cooperación regional a través de la Red Iberoamericana de Protección de Datos y la OEA, el fortalecimiento de los mecanismos de supervisión del Sistema Interamericano y la voluntad legislativa de los Estados de asumir las implicaciones regulatorias de su propia inserción en la economía digital global.

6. CONCLUSIÓN

La investigación permite afirmar que los marcos normativos, institucionales y procesales constitucionales vigentes en Colombia y Ecuador —y en buena parte de América Latina— resultan insuficientes para garantizar la protección efectiva de la memoria digital íntima frente a plataformas privadas, en los términos exigidos por los estándares del Sistema Universal e Interamericano de Derechos Humanos. La brecha no radica únicamente en la ausencia de normas, sino en la inadecuación de las categorías jurídicas disponibles para captar la especificidad de un fenómeno que desborda los esquemas regulatorios tradicionales.

A partir de estos hallazgos, se formulan las siguientes recomendaciones concretas. Para los legisladores: primero, incorporar en las leyes de protección de datos una definición específica de memoria digital íntima como categoría de protección reforzada, diferenciada de los datos personales y de los datos sensibles conforme a los criterios propuestos en la Tabla 1; segundo, establecer obligaciones de eliminación efectiva con plazos máximos verificables — no superiores a 30 días hábiles— y sanciones específicas por incumplimiento; tercero, incluir cláusulas de alcance extraterritorial que sometan a la jurisdicción nacional a toda plataforma que ofrezca servicios u obtenga datos de personas ubicadas en el país, siguiendo el modelo del artículo 3 del RGPD, de la LGPD brasileña y de la Ley 21.719 chilena; cuarto, dotar a las autoridades de control de recursos técnicos, financieros y humanos proporcionales al poder de los actores que deben supervisar; y quinto, regular la figura del habeas data colectivo o estructural como mecanismo procesal constitucional apto para abordar vulneraciones sistémicas de la memoria digital íntima por parte de plataformas.

Para las plataformas: adoptar mecanismos verificables de eliminación real de datos — no solo la desactivación de cuentas—, implementar evaluaciones de impacto en derechos humanos conforme a los Principios Rectores de Naciones Unidas, y garantizar que las políticas de retención respondan a los principios de finalidad y minimización. Para los usuarios: ejercer de manera informada los derechos de acceso, rectificación, cancelación y portabilidad; configurar activamente las opciones de privacidad; y participar en los procesos de consulta ciudadana sobre regulación digital.

Se identifican tres líneas de investigación futura que podrían profundizar los aportes del presente estudio: primera, el diseño procesal del habeas data colectivo frente a plataformas transnacionales, incluyendo cuestiones de legitimación activa, competencia jurisdiccional y ejecución de sentencias; segunda, la evaluación empírica de la eficacia de las autoridades nacionales de protección de datos en América Latina, mediante indicadores cuantitativos de gestión, sanción y cooperación internacional; y tercera, el análisis de la intersección entre memoria digital íntima e inteligencia artificial generativa, en la medida en que los modelos de lenguaje de gran escala se entrenan con datos personales cuya eliminación efectiva plantea desafíos técnicos y jurídicos inéditos. Las recomendaciones formuladas requieren desarrollo legislativo detallado que excede el alcance del presente artículo, pero el texto proporciona los fundamentos jurídicos, comparados y procesales constitucionales para orientar dicho desarrollo.

7. BIBLIOGRAFÍA

- Aristizábal Correa, D. A. (2019). Derecho al olvido digital en Colombia: retos contemporáneos en una sociedad. *Justicia*, 24(36), 211–225.
<https://doi.org/10.17081/just.24.36.3766>
- Asamblea Nacional Constituyente de Colombia. (1991). *Constitución Política de Colombia*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125>
- Balkin, J. M. (2016). Information fiduciaries and the First Amendment. *UC Davis Law Review*, 49(4), 1183–1234. https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>
- Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
<https://doi.org/10.1093/oso/9780190246693.001.0001>
- Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012. *Diario Oficial* 48.587. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Congreso de la República de Colombia. (2021). Ley 2157 de 2021. *Diario Oficial* 51.842.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=173246>
- Congreso de la República de Colombia. (2023). Ley 2300 de 2023. *Diario Oficial* 52.464.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=213628>
- Corte Constitucional de Colombia. (2004). Sentencia T-025/04 [M.P. Manuel José Cepeda Espinosa]. <https://www.corteconstitucional.gov.co/relatoria/2004/t-025-04.htm>
- Corte Constitucional de Colombia. (2015). Sentencia T-277/15 [M.P. María Victoria Calle Correa]. <https://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm>
- Corte Constitucional de Colombia. (2019). Sentencia SU-420/19 [M.P. José Fernando Reyes Cuartas]. <https://www.corteconstitucional.gov.co/relatoria/2019/su420-19.htm>
- Corte Interamericana de Derechos Humanos. (2009). Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009. Serie C No. 200.
https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf
- Guerrero, A. F. (2025). Neuroderechos en Colombia: autodeterminación informativa, integridad e identidad mental ante las neurotecnologías. *Prolegómenos*, 28(55), 13–22. <https://doi.org/10.18359/prole.7135>
- Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.

- Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press. <https://press.princeton.edu/books/paperback/9780691150369/delete>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–158. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>
- Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2018). El derecho a la privacidad en la era digital (A/HRC/39/29). <https://undocs.org/en/A/HRC/39/29>
- Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2021). El derecho a la privacidad en la era digital (A/HRC/48/31). <https://www.ohchr.org/en/privacy-in-the-digital-age>
- Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press. <https://doi.org/10.4159/9780674246874>
- Puccinelli, O. R. (2004). Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. *Vniversitas*, 53(107), 471–501. <https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/14792>
- Remolina Angarita, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana de Derecho Internacional*, 8(16), 489–524. <https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/13847>
- Remolina Angarita, N. (2013). *Tratamiento de datos personales: Aproximación internacional y comentarios a la Ley 1581 de 2012*. Legis.
- Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza. <https://www.laterza.it/scheda-libro/?isbn=9788858119303>
- Rojas, B. M. (2020). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus*, 8(1), 107–139. <https://novumjus.ucatolica.edu.co/article/view/652>
- Ruggie, J. G. (2011). *Principios Rectores sobre las empresas y los derechos humanos* (A/HRC/17/31). Consejo de Derechos Humanos de las Naciones Unidas. <https://digitallibrary.un.org/record/705860>
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90(4), 1087–1155. <https://doi.org/10.2307/3481326>
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press. <https://www.hup.harvard.edu/books/9780674035072>

- Tantaleán Odar, R. M. (2016). Tipología de las investigaciones jurídicas. *Derecho y Cambio Social*, (43), 1–37. <https://dialnet.unirioja.es/servlet/articulo?codigo=5456267>
- Villabella Armengol, C. M. (2020). Los métodos en la investigación jurídica. Algunas precisiones. *Revista Jurídica Jalisciense*, (62), 161–188. <https://revistas.udal.cl/index.php/deam/article/view/79>
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>

Polo de Capacitación, Investigación y Publicación (POCAIP) hace constar que:

El artículo científico:

**"Memoria digital íntima y obligaciones estatales frente a plataformas privadas:
insuficiencias regulatorias y procesales constitucionales en América Latina."**

De autoría:

**DIEGO ANDRES DELGADO PRIETO, MARCELA YULIETH LÓPEZ CAICEDO y JOSÉ
ALEJANDRO VILLALTA LEÓN**

Habiéndose procedido a su revisión y analizados los criterios de evaluación realizados por lectores pares expertos (externos) vinculados al área de experticia del artículo presentado, ajustándose el mismo a las normas que comprenden el proceso editorial, se da por aceptado

la publicación en el **Vol. 11, No 5, junio-agosto 2026**, de la revista Dominio de las Ciencias, con ISSN 2477-8818, indexada y registrada en las siguientes bases de datos y repositorios: **Clase, Erihplus, Latindex, MIAR, I2OR, Google Académico, OAJI, LatAm Studies, SIS, SJIF, ESJI, Issuu, Scribd, Calaméo e Internet Archive, WorldCat, Base.**

Y para que así conste, firmo la presente en la ciudad de Manta, a los 14 días del mes de junio del año 2026.



Abg. Néstor Darío Suárez Montes
DIRECTOR

Polo de Capacitación, Investigación y Publicación (POCAIP) hace constar que: