RIDI
Revista de Investigación
Desarrollo e Innovación

Estado actual de la protección de datos en el ecosistema digital colombiano

Current status of data protection in the Colombian digital ecosystem

Artículo de investigación

Recibido: febrero 21 de 2025
Aceptado: junio 25 de 2025
Publicado: agosto 15 de 2025

Cómo citar este artículo: Araq ue-Chacón, A. C., Pardo-García, A., & Becerra-Galvis, Z. Y. (2025). Estado actual de la protección de datos en el ecosistema digital colombiano. *Revista de Investigación, Desarrollo e Innovación, 15*(2), 405-422.

doi: https://doi.org/10.19053/uptc.20278306.v15.n2.2025.19911

Andrea Carolina Araque-Chacón
Universidad de Pamplona, Pamplona, Colombia.
E-mail: acaraque@unipamplona.edu.co
Orcid: https://orcid.org/0000-0003-0816-0458

Aldo Pardo-García*
Institución de Pamplona, Pamplona, Colombia.
E-mail: apardo13@unipamplona.edu.co
Orcid: https://orcid.org/0000-0003-2040-9420

Zaidly Yurley Becerra-Galvis
Universidad de Manizales, Manizales, Colombia.
E-mail: zbecerra113720@umanizales.edu.co
Orcid: https://orcid.org/0009-0009-4893-4957

Resumen

La investigación analiza la efectividad del marco legal colombiano en la protección de datos personales frente a los desafíos planteados por tecnologías emergentes, como la inteligencia artificial, el Big Data, la tecnología blockchain y el internet de las cosas. A través de una revisión jurídica y documental, se identificaron limitaciones significativas en la aplicación de la Ley 1581 de 2012, que establece principios para la protección de datos en Colombia. Los resultados revelan que, aunque el país cuenta con un marco normativo relevante, existen vacíos que dificultan una protección efectiva de la privacidad en el contexto digital. Se destaca la necesidad de fortalecer la supervisión por parte de las autoridades, actualizar la normativa para abordar los riesgos tecnológicos y fomentar una mayor conciencia social sobre los derechos digitales. Las conclusiones sugieren acciones específicas para optimizar la regulación y garantizar una protección más robusta de los datos personales en Colombia.

Palabras clave: datos personales, inteligencia artificial, marco legal, privacidad.

Abstract

This study examines the effectiveness of Colombia's legal framework in safeguarding personal data against the challenges posed by emerging technologies, such as artificial intelligence, Big Data, blockchain, and the Internet of Things. Through a legal and documentary review, significant limitations were identified in the implementation of Law 1581 of 2012, which establishes principles for data protection in Colombia. The findings reveal that although the country has a relevant regulatory framework, there are gaps that hinder effective privacy protection in the digital context. The study underscores the need to strengthen oversight by regulatory authorities, update legislation to address technological risks, and promote greater societal awareness of digital rights. The conclusions propose specific actions to enhance regulation and ensure more robust protection of personal data in Colombia.

Keywords: personal data, artificial intelligence, legal framework, privacy.

1. Introducción

En el contexto digital actual, el derecho a la privacidad ha adquirido una relevancia crucial debido al avance tecnológico y la recopilación masiva de datos personales por parte de entidades privadas y gobiernos. Según Arana (2024), esta recopilación se realiza a través de redes sociales, aplicaciones, transacciones en línea, tecnologías de rastreo como cookies y datos demográficos, lo que plantea serios dilemas sobre la seguridad y el respeto a la intimidad. Además, se debate hasta qué punto las instituciones y corporaciones pueden administrar datos personales sin comprometer la dignidad y autonomía de los individuos.

Por su parte, Belzuz (2024) destaca que herramientas como la inteligencia artificial y el reconocimiento facial, aunque ofrecen servicios personalizados y agilidad, también requieren niveles de vigilancia sin precedentes, lo que exige una regulación clara que equilibre la innovación tecnológica con la protección de datos. Asimismo, normativas como el Reglamento General de Protección de Datos (RGPD), del Parlamento Europeo & Consejo Europeo (2016), buscan establecer estándares, aunque enfrentan desafíos de implementación en un entorno dinámico.

En este sentido, Ariza et al. (2020) y Moreno (2021) enfatizan en la necesidad de fomentar una conciencia social sobre la protección de datos, responsabilizando a los gobiernos de garantizar transparencia y promover políticas que prioricen la privacidad. En Colombia, la Ley 1581 de 2012 y otras normativas buscan proteger los datos personales bajo principios de legalidad, seguridad y transparencia, supervisadas por la Superintendencia de Industria y Comercio (SIC). Sin embargo, Cabezas-Azuero (2023) señala que el rápido avance tecnológico, especialmente en Inteligencia Artificial (IA) y big data, exige una constante actualización de las regulaciones para mantener su eficacia.

Desde una perspectiva teórica, el derecho a la privacidad se fundamenta en principios de libertad y autonomía, siendo clave para el ejercicio de los derechos humanos. La Oficina del Alto Comisionado para los Derechos Humanos (OHCHR, 2024), destaca la necesidad de un marco legal que se ajuste a los avances tecnológicos para garantizar la protección de datos personales y los derechos digitales. En Colombia, pese al marco legal existente, persisten vacíos que dificultan la protección total de la privacidad digital. Sánchez (2023) destaca la necesidad de una cultura que valore estos derechos, impulsando el uso legal de la información. Además, Cano (2018) identifica desafíos como: escasez de recursos, falta de capacitación y necesidad de vigilancia para fortalecer la normativa existente.

Lo anterior conduce a la siguiente pregunta: ¿En qué medida las regulaciones actuales, como la Ley 1581 de 2012, abordan los riesgos de las nuevas tecnologías para la protección de datos en el ecosistema digital colombiano? Los objetivos de la investigación incluyen: identificar y analizar los principales elementos de la Ley Estatutaria 1581 de 2012 y su impacto en la protección de datos personales en

Colombia; examinar el papel de la Superintendencia de Industria y Comercio (SIC) en la regulación y supervisión del cumplimiento normativo; y valorar los desafíos actuales que enfrenta la normativa colombiana en el contexto de la recolección masiva de información personal y el uso de nuevas tecnologías.

2. Metodología

Esta investigación se enmarca dentro de un enfoque cualitativo, con un diseño documental y doctrinal, orientado al análisis crítico de la normativa vigente sobre la protección de datos personales en Colombia. Para ello, se llevó a cabo una revisión exhaustiva de fuentes primarias y secundarias, seleccionadas con base en su relevancia, actualidad y pertinencia frente al objeto de estudio.

Entre las fuentes primarias consultadas, se destacan: La Ley Estatutaria 1581 de 2012, que regula el tratamiento de datos personales en Colombia (Congreso de la República de Colombia, 2012).); Los Decretos Reglamentarios 1377 de 2013 y 886 de 2014, que desarrollan aspectos específicos de dicha ley; Resoluciones emitidas por la Superintendencia de Industria y Comercio (SIC), autoridad nacional en protección de datos, en especial aquellas que resuelven casos relevantes de los últimos tres años; Jurisprudencia de la Corte Constitucional y del Consejo de Estado, en relación con el derecho a la privacidad y el hábeas data.

Mientras que, como fuentes secundarias, se incluyeron artículos académicos publicados en revistas especializadas de derecho público y nuevas tecnologías, estudios de caso elaborados por observatorios jurídicos y centros de investigación, como el Observatorio de Derecho Informático Colombiano (ODIC) y el Centro de Estudios de Derecho Informático de la Universidad Externado de Colombia; informes técnicos de la SIC y publicaciones institucionales del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La recolección de información se centró en el análisis documental de textos normativos, doctrinales y casos prácticos relacionados con la aplicación de la legislación colombiana en materia de protección de datos. Esta etapa incluyó la identificación de decisiones sancionatorias relevantes proferidas por la SIC, que ilustran los retos actuales de implementación normativa y el nivel de cumplimiento por parte de los responsables del tratamiento de datos.

Adicionalmente, se realizó un análisis comparativo entre la legislación colombiana y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, con el fin de identificar similitudes, diferencias y posibles aprendizajes para el fortalecimiento del régimen colombiano. Este análisis se apoyó en estudios jurídicos internacionales y documentos oficiales de la Comisión Europea y del Comité Europeo de Protección de Datos y en investigaciones como la de Chaparro (2014), entre otras, que permitió realizar ese comparativo.

Los criterios de selección de los documentos y casos analizados respondieron

a su actualidad (publicaciones de los últimos tres años), relevancia temática y aplicabilidad directa al contexto colombiano. Se priorizaron aquellas fuentes que ofrecen una visión integral de los desafíos normativos y operativos que enfrenta el país en la garantía efectiva del derecho a la protección de datos personales.

3. Resultados y discusión

3.1 El derecho a la privacidad y los datos personales

El derecho a la privacidad es fundamental para proteger la dignidad y libertad individual, especialmente en una sociedad digital donde la exposición de datos es constante. Como indican Díaz-Alabart (2024) y Bertoni (2016), la digitalización exige una gobernanza adecuada de la ciudadanía digital, lo que implica ajustes jurídicos como señala Orza-Linares (2011).

Según Estrada (2003), la privacidad otorga a cada persona control sobre su información personal, protegiéndola de intromisiones sin consentimiento y este derecho garantiza que cada individuo decida quién accede a sus datos y bajo qué condiciones, lo que resulta esencial para la libertad y la dignidad humana.

A nivel internacional, la Declaración Universal de los Derechos Humanos (DUDH), de la Organización de las Naciones Unidas (ONU, 1984) y el Convenio Europeo de Derechos Humanos (CEDH) (Consejo de Europa, 1950), reconocen el derecho a la vida privada; el artículo 12 de la DUDH prohíbe injerencias arbitrarias en la vida personal, y el artículo 8 del CEDH establece que las autoridades no deben intervenir, salvo por razones justificadas como la seguridad nacional.

El Reglamento General de Protección de Datos (RGPD) de la UE (Parlamento Europeo & Consejo Europeo, 2016) regula el tratamiento de datos personales, exigiendo consentimiento y condiciones claras para su uso; establece figuras como el responsable y encargado del tratamiento, así como derechos para los titulares: acceso, rectificación, supresión, oposición, entre otros. Además, exige notificar violaciones de seguridad y promueve la privacidad desde el diseño.

Los datos personales incluyen información identificable (nombre, dirección), biométrica (huellas, reconocimiento facial), y derivados del uso digital (navegación, redes sociales). Algunos, como los de salud o ideología, requieren protección reforzada.

Organismos como la ONU y la OCDE, han promovido marcos éticos para el tratamiento de datos, por ejemplo, destaca que la protección debe ser proporcional a la sensibilidad de los datos. Y, además en entornos digitales, el uso inadecuado de información puede derivar en violencias, como la violencia de género digital, reconocida por la Organización de Estados Americanos (OEA, 2022), que se manifiesta mediante acoso, amenazas y difusión de contenido sin consentimiento.

Rojas (2017) clasifica los datos en públicos, semiprivados y privados, con distin-

tos niveles de protección. Mientras que Ariza et al. (2020), resaltan principios clave en el tratamiento de datos: transparencia, finalidad y minimización, y que el aumento de dispositivos conectados intensifica la necesidad de actualización normativa, dado que se estima que para 2025 habrá 75 mil millones de dispositivos, lo que incrementa el flujo de datos y los riesgos asociados.

Asimismo, tecnologías como el *blockchain* y el *cloud computing* ofrecen ventajas en la gestión de información, pero también presentan desafíos éticos y de control, especialmente en cuanto a la eliminación de datos y la seguridad delegada a terceros, como asegura Lecuit (2019).

3.2 Desafíos de las nuevas tecnologías a la protección de datos

En la era digital, herramientas como redes sociales, aplicaciones móviles, Inteligencia Artificial (IA), *Big Data, blockchain* e Internet de las cosas (IoT) han transformado radicalmente las formas de interacción, circulación y tratamiento de la información personal (Benítez-Arrieta & Cantillo-Velásquez, 2025). Esta exposición constante ha dado lugar a lo que Lévano y Porchia (2023) denominan la "cultura del anonimato", caracterizada por el uso de identidades ficticias, alias o avatares que, si bien pueden fomentar la igualdad en la expresión, también facilitan prácticas como el *trolling*, la suplantación de identidad o la manipulación mediante *bots*.

El procesamiento de datos personales es hoy un eje central de la economía digital. Según Sánchez (2023), esta realidad demanda una reflexión ética y legal profunda sobre la responsabilidad de quienes recolectan y utilizan dicha información, especialmente cuando los avances tecnológicos superan el alcance de la normativa vigente, generando tensiones con los derechos fundamentales. La inteligencia artificial, por ejemplo, emplea grandes volúmenes de datos sensibles para tomar decisiones automatizadas (Puentes-Aguillón et al., 2025). Morales (2020) advierte que, sin marcos regulatorios robustos, esto puede derivar en riesgos significativos como la discriminación algorítmica, evidenciada en casos como el de *Google Photos* (2015) o el *chatbot Tay* de *Microsoft*.

Otro fenómeno creciente es la perfilación digital, práctica que rastrea la actividad del usuario para crear perfiles conductuales con fines comerciales o delictivos. Esta técnica, señala Sánchez (2023), puede facilitar delitos como el ciberacoso, la extorsión o la violencia digital, especialmente contra mujeres y grupos vulnerables. Por ello, es fundamental que el uso de tecnologías emergentes respete principios como la legalidad, el consentimiento informado y la finalidad específica del tratamiento de datos. A estos se suman otros principios derivados, como la proporcionalidad, la seguridad, la calidad y la protección efectiva, según Morales (2020).

La automatización y la inteligencia artificial también presentan riesgos sociales más amplios. Clúa de Yarza (2020) advierte sobre el impacto de la auto-

matización en el empleo, subrayando la necesidad de garantizar una gestión ética y segura de los datos personales en entornos laborales digitalizados. Por su parte, Aristizábal (2019) plantea que una verdadera protección de datos requiere no solo marcos legales sólidos, sino sistemas funcionales de autorregulación, con compromisos gubernamentales efectivos. Destaca también el derecho al olvido como una garantía esencial frente al tratamiento masivo y permanente de la información digital.

Como expone Mendivelso (2024), el control de la información se ha convertido en una forma de poder. Grandes corporaciones y conglomerados, muchas veces ocultos tras el anonimato digital, gestionan y manipulan datos personales con fines lucrativos o estratégicos, sin que los titulares tengan control real sobre el destino de su información. Este panorama exige, más que nunca, una regulación estricta y mecanismos eficaces para evitar que las tecnologías, lejos de garantizar derechos, los vulneren.

3.3 Normativa vigente en Colombia

Colombia reafirma su compromiso con la protección de los datos personales a nivel nacional mediante el artículo 15 de la Constitución Política de Colombia (1991), que garantiza el derecho a la intimidad, la vida privada y la buena reputación. Este artículo impone al Estado la obligación de respetar y hacer cumplir dichas garantías, además de reconocer el derecho de los ciudadanos a acceder, actualizar y rectificar la información recopilada sobre ellos en bases de datos públicas o privadas.

La normativa nacional también asegura la inviolabilidad de las comunicaciones privadas, salvo en circunstancias excepcionales bajo orden judicial. Para robustecer este derecho, el país ha adoptado un marco normativo que incluye:

La Ley 1266 de 2008, que regula el Habeas Data en el ámbito crediticio; La Ley 1581 de 2012, que establece el régimen general de protección de datos personales; La Ley 1273 de 2009, que introduce delitos informáticos y protege la información digital; y la Ley 1712 de 2014, que garantiza el acceso a la información pública, protegiendo los datos sensibles.

Este conjunto normativo busca armonizar el derecho a la privacidad con los principios de acceso a la información y seguridad nacional, promoviendo un uso responsable y transparente de los datos personales.

Las leyes colombianas, reforzadas por jurisprudencia de la Corte Constitucional, fortalecen el derecho a la privacidad, incluyendo la inviolabilidad del domicilio y de las comunicaciones. Un ejemplo representativo es la Sentencia C-308 de 2019, que evaluó el artículo 33 de la Ley 1801 de 2016 (Código Nacional de Policía y Convivencia), en donde la Corte avaló el ingreso a domicilios sin orden judicial únicamente en casos de "imperiosa necesidad" como emergencias o rescates, estableciendo que dicha excepción debe aplicarse de manera

restrictiva y proporcional (Corte Constitucional de Colombia, 2019).

Además, la Corte ha sostenido que toda intervención en estos derechos debe ser justificada, respetando la dignidad y autonomía del titular de los datos. Por ejemplo, Basto y Salcedo (2014) proponen que el Estado puede acceder a documentos privados para fines fiscales o de inspección, siempre dentro de los límites establecidos por la ley.

En un entorno digital, donde la generación de huellas en línea es constante (a través de redes sociales, plataformas digitales, etc.), el derecho a la privacidad se vuelve aún más crucial. Este permite a las personas controlar el acceso a su información, limitando su uso no autorizado y resguardando su integridad.

No obstante, a pesar de los avances normativos, persisten vacíos legales que dificultan una protección integral. Muchas empresas carecen de los recursos o conocimientos para implementar mecanismos adecuados de seguridad. Un caso preocupante es el del SECOP (Sistema Electrónico para la Contratación Pública), donde datos sensibles como cédulas, hojas de vida y estados financieros están expuestos, aunque el principio de publicidad ampara esta práctica, la ausencia de filtros adecuados puede vulnerar derechos fundamentales.

Desde una perspectiva legal, la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012, art. 4) establece principios rectores como la confidencialidad, finalidad y proporcionalidad. Sin embargo, la disponibilidad de información mediante identificadores como la cédula puede contradecir el principio de minimización de datos, que busca limitar la recolección y divulgación al mínimo necesario para un fin determinado.

El Sistema Electrónico para la Contratación Pública (SECOP), aunque promueve la transparencia en la contratación estatal colombiana, carece de mecanismos de autenticación y verificación de propósito, lo que abre la puerta al uso indebido de información personal. Por ello, se hace urgente reforzar los protocolos de seguridad y establecer medidas que equilibren el derecho al acceso a la información con la protección de datos sensibles.

En marzo de 2023, Colombia suscribió la Carta de Principios y Derechos Digitales, junto a otros países de la región, siendo un instrumento que busca estandarizar la protección de los derechos digitales y adaptar las normativas a la era de la información, y su implementación representa un avance hacia un ecosistema digital más seguro, alineado con las mejores prácticas internacionales.

3.4 La Ley 1581 de 2012 y el rol de la SIC

La Ley 1581 de 2012, conocida como Ley de Protección de Datos Personales, regula el tratamiento de datos conforme al derecho a la privacidad consagrado en el artículo 15 constitucional, siendo norma que garantiza a los titulares el derecho a conocer, actualizar y rectifi-

car su información, y se fundamenta en principios como: Legalidad dado que el tratamiento debe ceñirse a lo establecido por la ley; la libertad que requiere consentimiento libre, previo y expreso; y la seguridad que se impone medidas técnicas y administrativas de protección.

La entidad encargada de hacer cumplir esta ley es la Superintendencia de Industria y Comercio (SIC). Entre sus funciones se encuentran: supervisar la recolección y tratamiento de datos personales; garantizar la información clara a los titulares; proteger especialmente los datos sensibles; prohibir, salvo excepciones legales, el tratamiento de datos de menores; e investigar y sancionar violaciones mediante multas y medidas correctivas, citado en Cabezas-Azuero (2023). Además, emite directrices (no siempre vinculantes) para orientar el uso responsable de los datos, y supervisa el cumplimiento del Decreto 1377 de 2013, que reglamenta parcialmente la Ley 1581.

Sin embargo, la implementación de esta ley enfrenta múltiples desafíos. A diferencia del Reglamento General de Protección de Datos (RGPD) europeo, Colombia no exige evaluaciones de impacto ni pruebas de cumplimiento, y permite el tratamiento bajo "interés legítimo", lo que puede debilitar la protección. La falta de formación técnica y pedagógica en entidades públicas, sumada a una débil fiscalización, limita la efectividad del marco legal.

Un ejemplo de estas debilidades es la aplicación CoronApp, desarrollada durante la pandemia, que recopiló datos sin el debido consentimiento, facilitando su uso potencialmente indebido. Así lo evidenció un foro académico organizado por la Universidad Externado de Colombia que fue recopilado por Quiñones (2022), concluyendo que la Ley 1581 es insuficiente ante los retos de la automatización, el control algorítmico y la transferencia internacional de datos.

Aunque el sector privado ha mostrado avances en pedagogía y cumplimiento, el Estado aún presenta rezagos importantes, en el que el fortalecimiento normativo y la implementación efectiva de la Carta de Principios y Derechos Digitales podrían impulsar una reforma legal integral, más acorde con los desafíos contemporáneos.

En consecuencia, si bien la Ley 1581 de 2012 ha sido un hito para la protección de datos en Colombia, se requieren reformas urgentes en aspectos como: Clarificación del consentimiento expreso y mecanismos de validación; Regulación de tecnologías emergentes (*IA, Big Data, blockchain*); Establecimiento de directrices de la SIC con carácter obligatorio; Fortalecimiento de la supervisión y sanción; y la regulación clara sobre transferencias de datos interinstitucionales e internacionales.

3.5 Algunos casos colombianos relacionados con la protección de datos y el derecho a la privacidad

En Colombia, la protección de los datos personales enfrenta múltiples desafíos

estructurales y prácticos. A pesar de la existencia de un marco normativo robusto, como la Ley 1581 de 2012, persisten vulneraciones frecuentes al derecho a la privacidad. Según datos citados por la relatora de la ONU, Ana Brian Nougrères, la Superintendencia de Industria y Comercio (SIC) recibe en promedio 2.300 quejas mensuales por infracciones en el tratamiento de datos, lo que evidencia una deficiente aplicación de las normas vigentes (Remolina, 2023).

Entre las problemáticas más comunes reportadas, de acuerdo con Mesa (2015), se encuentran: llamadas comerciales no solicitadas, reportes crediticios incorrectos e intentos de estafa. Estas prácticas indican no solo el uso indebido de los datos, sino también una falta de conocimiento de la ciudadanía sobre sus derechos, lo que limita la interposición de denuncias y genera un subregistro significativo.

La relatora Nougrères (2021), ha insistido en la necesidad de educar a las personas sobre los riesgos de una gestión inadecuada de sus datos y la importancia de prácticas básicas como la lectura de términos y condiciones de privacidad. En la misma línea, la profesora María Solange Maqueo Ramírez, del CIDE (México), advierte que, sin una cultura sólida de protección de datos, las normas resultan insuficientes. Señala que tanto el Estado como las empresas deben asumir un rol activo en la protección de la información, dada su influencia en derechos conexos como el acceso al crédito o a servicios de salud (Remolina, 2023).

Un caso emblemático es el fallo de la Corte Interamericana de Derechos Humanos (CIDH) del 18 de marzo de 2024, en el caso Miembros de la Corporación de Abogados José Alvear Restrepo (CAJAR) vs. Colombia. En este, la Corte reconoció el derecho a la autodeterminación informativa en contextos de vigilancia estatal, condenando a Colombia por interceptaciones ilegales, seguimiento, robo de datos y otras formas de vigilancia contra defensores de derechos humanos y sus familias, que derivaron incluso en desplazamientos forzados (Camacho, 2024).

El fallo estableció que las personas tienen derecho a conocer, corregir y eliminar la información recolectada por organismos de inteligencia, incluyendo la obtenida mediante actividades como el ciberpatrullaje. La Corte advirtió que prácticas de vigilancia digital sin control pueden violar gravemente el derecho a la privacidad, e instó a Colombia a depurar sus bases de datos y adoptar medidas concretas para garantizar un tratamiento ético y legal de la información (Camacho, 2024).

En el ámbito nacional, la SIC ha emitido múltiples sanciones por incumplimientos a la normativa de protección de datos. En 2019, sancionó al Banco Falabella (Resolución 9766 de 2019) y a Rappi S.A.S. (Resolución 9800 de 2019) por vulnerar el derecho de supresión y tratar datos sin autorización. El Banco Falabella incumplió solicitudes de eliminación de información personal y excedió ampliamente el plazo legal para responder. Rappi, por su parte, manejó datos sin verificación de identidad ni consentimiento, y envió comunicaciones no autorizadas,

lo que derivó en multas y medidas correctivas (SIC, 2019).

Más recientemente, en 2024, se documentaron casos que muestran un patrón de incumplimiento. La empresa Baguer S.A.S. fue sancionada (Resolución 1016 de 2024) por transferir datos sensibles a terceros sin consentimiento. La Clínica Nueva Sonrisa Calima S.A.S. fue sancionada por no implementar medidas de seguridad adecuadas (Resolución 1332 de 2024). En la Resolución 16851 (2024), la Fundación para el Desarrollo Integral del Sistema de Seguridad Social fue multada por no acreditar políticas de tratamiento de datos. Asimismo, Credivalores - Crediservicios S.A. recibió una sanción significativa (259 smlmv, Resolución 29069 de 2024) por reportar negativamente a titulares sin previa notificación (SIC, 2024a; 2024b; 2024c; 2024d).

Otros casos como el de Carlos Mario Soto Duque – Modas y Modas La Diagonal y Needish Colombia S.A.S., sancionados por no contar con autorización previa y políticas de tratamiento (Resoluciónes 31523 y 33982 de 2024), y Datsoft S.A.S., por consultar historiales crediticios sin consentimiento (Resolución 34528 de 2024), reafirman esta tendencia. En las Resoluciones 40286 y 41965 de 2024, se sancionó al Fondo de Empleados de Credibanco y al Foemiseg por incumplir requerimientos en políticas de tratamiento, seguridad y atención a reclamos, permitiendo incluso accesos no autorizados (SIC, 2024e; 2024f; 2024g; 2024h; 2024i).

Como señala Remolina (2023), no basta con consagrar el derecho a la privacidad en el ordenamiento jurídico; se requiere una implementación activa y un compromiso real por parte de las entidades encargadas del tratamiento de datos. La mayor parte de las sanciones en 2024 se relaciona con la falta de adopción de políticas adecuadas en almacenamiento, uso, circulación y supresión de datos personales.

Esto evidencia un desfase entre la normativa existente y su aplicación efectiva. Además, las nuevas tecnologías como la inteligencia artificial, el *big data*, la cadena de bloques (*blockchain*) y el internet de las cosas plantean desafíos complejos. La protección de los datos personales debe adaptarse a estos escenarios, considerando el riesgo de nuevas formas de vigilancia y explotación de la información.

Entonces, la efectividad del derecho a la protección de datos no reside únicamente en su regulación formal, sino en el cumplimiento efectivo de las obligaciones por parte de quienes tratan la información. La falta de conciencia de los titulares sobre sus derechos propicia un bajo nivel de denuncias y un elevado subregistro, debilitando el sistema de protección. La responsabilidad recae, en última instancia, en las organizaciones que deben garantizar la confidencialidad, seguridad y actualización de los datos recolectados (Morelos-Gómez et al., 2024).

3.6 Discusión

Los resultados permiten evaluar la hipótesis: aunque Colombia tiene un marco

legal para la protección de datos, existen vacíos que limitan su aplicación y afectan la privacidad digital. El análisis de leyes, estudios doctrinales y casos de la SIC revela que, pese a la Ley 1581 de 2012 y otras normativas, su implementación sigue presentando debilidades.

Respecto a la aplicabilidad de la ley y el respeto por la misma, se evidencia que en Colombia se incumplen las obligaciones de supresión y autorización de datos, y en general de protección de datos, reflejando una falta de cumplimiento práctico que la normativa no ha logrado controlar de forma efectiva. Estos casos y datos, como el de la CIDH, ilustran la dificultad de aplicar la normativa de forma exhaustiva y proteger adecuadamente los derechos de los ciudadanos, validando parcialmente la hipótesis.

Asimismo, la investigación señala que la regulación no ha avanzado al mismo ritmo que las nuevas tecnologías, como la IA, Big Data, tecnología blockchain e IoT, pues, la legislación actual carece de mecanismos específicos para abordar asuntos como consentimiento, regulación de entornos digitales, terminologías y nuevas formas de tratamientos, aplicación de sanciones, estipulación de responsabilidades claras a los responsables y encargados, exigencias de cargas y demostración de cumplimientos a las entidades responsables, estimación de riesgos y reglas para la transferencia de datos (Martínez, 2019). Lo anterior indica que existen grandes limitaciones para la protección completa de la privacidad digital, que distan en gran medida de los avances en términos de regulación de la Unión Europea.

Por lo tanto, los resultados confirman la validez de la hipótesis, señalando que, aunque el marco legal colombiano representa un avance importante, no es suficiente en su estado actual para enfrentar los desafíos tecnológicos y brindar una protección integral y eficaz de los datos personales.

Los resultados de esta investigación evidencian que, aunque Colombia cuenta con un marco legal para la protección de datos personales, representado principalmente por la Ley 1581 de 2012, existen vacíos y limitaciones significativas que dificultan una protección efectiva de la privacidad en el contexto digital. Estos hallazgos se alinean con la pregunta de investigación, que buscaba determinar en qué medida las regulaciones actuales abordan los riesgos asociados a las nuevas tecnologías emergentes.

En primer lugar, se observa que la Ley 1581 de 2012, aunque establece principios fundamentales como la legalidad, finalidad y seguridad en el tratamiento de datos, no ha evolucionado al ritmo de los avances tecnológicos. Esto se refleja en la falta de mecanismos específicos para abordar desafíos como el consentimiento expreso en entornos digitales, la portabilidad de datos, la transferencia internacional de información y la regulación de tecnologías emergentes. Estos vacíos normativos limitan la capacidad del marco legal colombiano para garantizar una protección integral de los datos personales, especialmente en un contexto donde la recolección y el análisis masivo de información se han vuelto omnipresentes.

En segundo lugar, la investigación revela que la Superintendencia de Industria y Comercio (SIC), encargada de supervisar el cumplimiento de la Ley 1581, enfrenta desafíos en su capacidad para aplicar sanciones y garantizar el cumplimiento de las normativas. Aunque se han impuesto multas a empresas por incumplimientos, como en los casos de Rappi y Banco Falabella, persisten prácticas recurrentes de manejo inadecuado de datos, lo que sugiere una falta de efectividad en la supervisión y una necesidad de fortalecer los mecanismos de control. Esto se relaciona con el marco teórico, que destaca la importancia de una supervisión robusta y adaptativa para garantizar la protección de los derechos digitales en un entorno tecnológicamente dinámico.

Además, los resultados muestran que la falta de conciencia social y educación sobre los derechos digitales contribuye a un subregistro de denuncias y a una baja tasa de cumplimiento por parte de las empresas. Esto coincide con lo expuesto por Camargo-Bedoya (2014), que enfatiza la necesidad de fomentar una cultura de protección de datos tanto en los ciudadanos como en las organizaciones. Desde esta perspectiva, la educación en derechos digitales se perfila como un componente crucial para empoderar a los ciudadanos y garantizar que ejerzan un control informado sobre su información personal.

En cuanto a las implicaciones prácticas, los hallazgos sugieren que Colombia debe avanzar hacia una actualización normativa que incorpore estándares internacionales, como los establecidos en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Esto incluiría la adopción de principios como el consentimiento expreso, la minimización de datos, la portabilidad y la obligación de notificar violaciones de seguridad en plazos específicos. Asimismo, se requiere una mayor inversión en recursos y capacitación para la SIC, con el fin de mejorar su capacidad de supervisión y aplicación de sanciones.

4. Conclusiones

El estudio evidenció que el marco legal colombiano en materia de protección de datos personales, pese a sus bases normativas, resulta insuficiente frente a los desafíos de la era digital. La Ley 1581 de 2012 presenta vacíos que comprometen el derecho a la privacidad, lo que exige una actualización normativa que responda a las tecnologías emergentes.

Se identificaron aportes relevantes del modelo europeo que podrían ser adaptados al contexto colombiano, como resaltan Bahamón y Barrero (2023): el consentimiento previo y expreso, la regulación específica para tecnologías como la IA, el Big Data y el IoT, y el fortalecimiento del rol de la Superintendencia de Industria y Comercio (SIC), como ente de vigilancia.

Asimismo, se destaca la necesidad de promover una educación en derechos digitales que permita a los ciudadanos ejercer un control informado sobre su información personal. Aunque existen

mecanismos regulatorios, su efectividad es limitada, por lo que se requiere una supervisión más robusta y una mayor claridad normativa para garantizar una protección de datos acorde con los estándares internacionales.

Contribución de los autores

Andrea Carolina Araque-Chacón: Metodología, Investigación, Redacción, Análisis formal.

Aldo Pardo-García: Metodología, Investigación, Redacción – revisión y edición.

Zaildy Yurley Becerra-Galvis: Metodología, Investigación, Redacción.

Implicaciones éticas

No existen implicaciones éticas por declarar en la escritura o publicación de este artículo.

Financiación

Los autores no recibieron recursos para la escritura o publicación de este artículo.

Conflictos de interés

No existen conflictos de interés de parte de los autores en la escritura o publicación de este artículo.

5. Referencias

Arana, A. (2024) La Privacidad de la información personal en la era digital. Al Poniente. https://alponiente.com/la-privacidad -de-la-informacion-personal-en-la-era-digital/

Ariza, J; Ayala, J., & González, L. (2020). La protección de datos en la era digital Colombia – España. Politécnico Gran Colombiano. https://hdl.handle.net/10823/2142

Aristizábal, D. (2019). Derecho al olvido digital en Colombia: Retos contemporáneos en una sociedad desactualizada. *Justicia, 24* (36), 1–15. https://doi.org/10.17081/JUST.24.36.3766

Bahamón, A., & Barrero, J. P. (2023). ¿Regulación o no para la IA? Propuesta de regulación híbrida en Colombia. *Revista Colombiana de Tecnologías de Avanzada, 2* (36), 27–33. https://doi.org/10.24054/rcta.v2i36.17

Basto, E., & Salcedo, S. (2014). Evaluación legal de la utilización de la inspección profunda de paquetes (DPI) en las redes de telecomunicaciones en Colombia. Universidad Inca Garcilaso de la Vega. http://intra.uigv.edu.pe/handle/20.500.11818/733

Belzuz, A. (2024). Derechos de privacidad en la era digital: Retos y soluciones legales. https://www.belzuz.net/es/publicaciones/en-espanol/item/11967-derechos-de-privacidad-en-la-era-digital-retos-y-soluciones-legales.html

Benítez-Arrieta, D. A., & Cantillo-Velásquez, I. M. (2025). Estrategias para facilitar la implementación de blockchain en la cadena de suministro de las PyMEs. *Revista de Investigación, Desarrollo e Innovación, 15* (1), 195-210. https://doi.org/10.19053/uptc.20278306.v15.n1.2025.19187

Bertoni, E. (2016). Internet y derechos humanos II: Aportes para la discusión de políticas públicas en América Latina. Ediciones del Jinete Insomne.

Cabezas-Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de la Facultad de Derecho y Ciencias Políticas, 53* (138). https://doi.org/10.18566/rfdcp.v53n138.a2

Camacho, L. (2024). Histórica sentencia de la Corte Interamericana de Derechos Humanos: La protección de datos aplica en las tareas de inteligencia. Derechos Digitales. https://www.derechosdigitales.org/24094/historica-sentencia-de-la-corte-interamericana-de-derechos-humanos-la-proteccion-de-datos-aplica-en-las-tareas-de-inteligencia/

Camargo-Bedoya, C. A. (2014). *S1581 solución informática de gestión de datos personales del ciudadano colombiano* (Tesis de maestría). Pontificia Universidad Javeriana, Colombia. https://doi.org/10.11144/javeriana.10554.15074

Cano, L. (2018). El panóptico digital de la protección de datos personales en Colombia. *Revista Temas,* 12, 125–140. https://doi.org/10.15332/RT.V0I12.2038

Clúa de Yarza, P. (2020). *El futuro del empleo: Los desafíos de la automatización, la inteligencia artificial y la robótica* (Trabajo fin de grado). Universidad Pontificia Comillas, España. https://hdl.handle.net/11531/37122

Congreso de la República de Colombia. (2012, octubre 17). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales (Diario Oficial No. 48.587). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Consejo de Europa. (1950). Convenio Europeo de Derechos Humanos. https://www.echr.coe.int/documents/d/echr/convention_spa

Constitución Política de Colombia. (1991). Diario Oficial No. 52.694 - 10 de marzo de 2024. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Corte Constitucional de Colombia. (2019, abril 12). Sentencia C-308/19 (José Fernando Reyes Cuartas, M. P.). https://www.corteconstitucional.gov.co/Relatoria/2019/C-308-19.htm

Chaparro, M. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. *Inventum, 9* (17), 32–37. https://doi.org/10.26620/UNIMINUTO.INVENTUM.9.17.2014.32-37

Díaz-Alabart, S. (2024). La tensión entre los derechos a la libre información y a la propia imagen en la era de internet. *Revista Cubana de Derecho, 4* (01), 442-465. https://revista.unjc.cu/index.php/derecho/article/view/274

Estrada, J. (2003). El derecho a la intimidad y su necesaria inclusión como garantía individual. http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Lecuit, J. (2019). La seguridad y la privacidad del blockchain, más allá de la tecnología y las criptomonedas. *Real Instituto Elcano.* https://www.realinstitutoelcano.org/analisis/la-seguridad-y-la-privacidad-del-blockchain-mas-alla-de-la-tecnologia-y-las-criptomonedas/

Lévano, G., & Porchia, M. (2023). Más que palabras: aspectos de la misoginia en línea. *Anuario de Filosofía del Derecho,* 38. https://doi.org/10.53054/afd.vi38.9742

Martínez, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial,* 27, 5–23. https://doi.org/10.18601/16571959.n27.01

Mendivelso, J. (2024). Seguridad y privacidad en el tiempo digital, la era de la información líquida. *Revista Científica Multidisciplinar, 8* (2). https://ciencialatina.org/index.php/cienciala/article/view/11136/16349

Mesa, A. (2015). La evidencia digital eximiente de violación a la protección del dato personal a partir de la autorregulación. *Academia y Virtualidad, 10*, 119–156. https://doi.org/10.18041/2215-8944/ACADEMIA.10.351

Morales, A. (2020). El impacto de la inteligencia artificial en la protección de datos personales. World Compliance Association. https://www.worldcomplianceassociation.com/2767/articulo-el-impacto-de-la-inteligencia-artificial-en-la-proteccin-de-datos-personales.html

Morelos-Gómez, J., Cardona-Arbeláez, D. A., & Lora-Guzmán, H. S. (2024). Digital transformation in the tourism sector: the key role of social networks. *Revista de Investigación, Desarrollo e Innovación, 14* (1), 27-40. https://doi.org/10.19053/20278306.v14.n1.2024.17284

Moreno, S. (2021). Privacidad y seguridad en tiempos digitales: ¿Por qué es importante leer la política de privacidad de tus aplicaciones? Noticias UNAD.

Nougrères, A. (2021). Colombia: El Sandbox sobre privacidad desde el diseño y por defecto en proyectos de inteligencia artificial. *Revista Latinoamericana de Protección de Datos Personales, 7,* 15. https://dialnet.unirioja.es/servlet/articulo?codigo=7778423

Oficina del Alto Comisionado para los Derechos Humanos (OHCHR). (2024). Normas internacionales relativas a la privacidad digital. https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

Organización de las Naciones Unidas, ONU. (1984). Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Organización de los Estados Americanos, OEA. (2022). La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta.

Orza-Linares, R. (2011). El derecho al anonimato en Internet. *TELOS: Cuadernos de Comunicación e Innovación, 89*, 24-33.

Parlamento Europeo & Consejo Europeo. (2016). Reglamento general de protección de datos: Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

Puentes-Aguillón, O. E., Fernández-Morales, F. H., & Niño-Vega, J. A. (2025). La inteligencia artificial y sus posibilidades en la educación básica: una experiencia con docentes en ejercicio. *Gestión y Desarrollo Libre, 10* (19). https://doi.org/10.18041/2539-3669/gestion_libre.19.2025.12738

Quiñones, D. (2022). ¿10 años de la ley de protección de datos: ¿Qué tanto hemos avanzado? ¿Qué nos hace falta? La ley al

tablero. https://www.uexternado.edu.co/wp-content/uploads/2024/02/10-ANOS-DE-LA-LEY-DE-PROTECCION-DE-DATOS-1.pdf

Remolina, N. (2023). Cada día, en Colombia se presentan cerca de 79 casos de violación de protección de datos personales. Universidad de los Andes.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus, 8* (1), 107–139. https://doi.org/10.14718/NOVUMJUS.2014.8.1.6

Sánchez, M. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo, 10* (1), e235. https://doi.org/10.14409/redoeda.v10i1.12626

Superintendencia de Industria y Comercio, SIC. (2019). Rappi y Banco Falabella sancionados por incumplir Ley de Protección de Datos. https://www.sic.gov.co/Rappi-y-Banco-Falabella-sancionados-por-incumplir-Ley-de-Proteccion-de-Datos

Superintendencia de Industria y Comercio, SIC. (2024a). Resolución 1016 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://sedeelectronica.sic.gov.co/sites/default/files/normativa/Resolucion_1016_de_2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024b). Resolución 1332 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://sedeelectronica.sic.gov.co/sites/default/files/normativa/RE1532-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024c). Resolución 16851 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://sedeelectronica.sic.gov.co/sites/default/files/normativa/RE16851-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024d). Resolución 29069 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE29069-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024e). Resolución 31523 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE31523-%202024.pdf

Superintendencia de Industria y Comercio, SIC. (2024f). Resolución 33982 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE33982-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024g). Resolución 34528 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE34528-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024h). Resolución 40286 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE40286-2024.pdf

Superintendencia de Industria y Comercio, SIC. (2024i). Resolución 41965 "Por la cual se impone una sanción y se imparten órdenes administrativas". https://www.sic.gov.co/sites/default/files/files/Normativa/RE41965-2024.pdf