Convicciones |vol. 12, no. 24, pp. 178-182 |Julio-Diciembre 2025 |E-ISSN 2385-7589

Desprotección Silenciosa: Una Reflexión Sobre Vigilancia, Datos Personales, Redes Sociales y Límites Institucionales

Silent Unprotection: A Reflection on Surveillance, Personal Data, Social Networks, and Institutional Limits

1. Wendy Michelle Rosado Quintero
2. Laura Manzano

Recibido: 12-09-2024
Aprobado: 23-12-2024

Resumen

El artículo reflexiona sobre la protección del derecho a la intimidad, el habeas data y la autodeterminación informativa en Colombia frente al avance de las tecnologías de vigilancia, las redes sociales y el tratamiento masivo de datos personales. A partir de referentes doctrinales como Solove y Nissenbaum, así como de normas nacionales y pronunciamientos constitucionales recientes, se examinan los riesgos derivados de la recolección, procesamiento, difusión e invasión de información personal. El análisis muestra que, aunque Colombia cuenta con la Ley 1581 de 2012 y la Ley 1266 de 2008, persisten límites institucionales para enfrentar la velocidad de las plataformas digitales, la videovigilancia y el perfilamiento algorítmico. Se concluye que la protección de datos requiere educación digital, supervisión técnica, transparencia y una cultura ciudadana que reconozca la privacidad como condición para la libertad, la dignidad y la participación democrática.

Palabras clave: intimidad, protección de datos, habeas data, redes sociales, vigilancia, privacidad digital

Abstract

This article reflects on the protection of the right to privacy, habeas data, and informational self-determination in Colombia in the face of the expansion of surveillance technologies, social networks, and mass processing of personal data. Drawing on doctrinal references such as Solove and Nissenbaum, as well as national regulations and recent constitutional decisions, it examines the risks arising from the collection, processing, dissemination, and invasion of personal information. The analysis shows that, although Colombia has Law 1581 of 2012 and Law 1266 of 2008, institutional limits persist in responding to the speed of digital platforms, video surveillance, and algorithmic profiling. It concludes that data protection requires digital education, technical oversight, transparency, and a civic culture that recognizes privacy as a condition for freedom, dignity, and democratic participation.

Keywords: privacy, data protection, habeas data, social networks, surveillance, digital privacy

Programa de Derecho. [Dato pendiente por completar] [Dato pendiente por completar] Universidad Francisco de Paula Santander, Ocaña, Colombia
Programa de Derecho. [Dato pendiente por completar] [Dato pendiente por completar] Universidad Francisco de Paula Santander, Ocaña, Colombia

***Autor de Correspondencia: [Dato pendiente por completar]**

Introducción

La discusión sobre el derecho a la intimidad y a la protección de datos personales ha adquirido un peso bastante fuerte en los últimos años, discusión que también ha tomado relevancia en nuestro país donde el uso de tecnologías de vigilancia, la presencia de grandes plataformas digitales y la falta de educación ciudadana sobre estos riesgos son cada vez más constantes. El derecho a la intimidad es reconocido por nuestra constitución desde 1991, y además está acompañado de importantes garantías fundamentales que buscan precisamente la protección de este derecho tales como el habeas data, y la autodeterminación informativa. Sin embargo, su aplicación práctica parece avanzar más lento que los sistemas de recolección masiva de información que actualmente usan tanto actores privados como públicos. En ese caso, no se trata solo de un asunto técnico, sino que detrás de la recopilación de datos hay relaciones de poder, desigualdades y prácticas que transforman la vida cotidiana, hoy más que nunca.

La lectura de diferentes autores en el campo de la privacidad permite ver que el problema es más complejo que simplemente "guardar" datos; el panorama se amplía cuando observamos que además de guardarlos implica también comprender cómo se usan, qué efectos tienen y quién controla sus flujos.

Metodología

El artículo se desarrolló mediante una revisión documental y reflexiva de carácter jurídico-analítico, centrada en doctrina especializada, normativa colombiana y jurisprudencia constitucional relacionada con el derecho a la intimidad, el habeas data y la protección de datos personales. La revisión consideró aportes teóricos sobre privacidad, integridad contextual, vigilancia y tratamiento de datos, así como normas nacionales como la Ley 1581 de 2012 y la Ley 1266 de 2008. La información fue organizada mediante análisis temático, identificando categorías como recopilación, procesamiento, difusión, invasión, vigilancia institucional, redes sociales, consentimiento informado, límites estatales y educación digital.

Resultados y discusión

Al leer a Daniel Solove, (2006) por ejemplo, especialmente en su libro A Taxonomy Of Privacy y varios de sus artículos previos, se nota que su aporte no es solo conceptual sino metodológico. Él critica que durante décadas los juristas trataron la privacidad como una especie de concepto difuso, casi emocional, muy difícil de definir. Su intención entonces fue organizar todo ese caos y mostrar que la privacidad no es una sola cosa, sino un conjunto de prácticas, riesgos y daños que se manifiestan de distintas formas. Esa postura es interesante porque rompe con la visión tradicional donde la privacidad se mide únicamente en términos de "se reveló o no se reveló información personal".

Solove desarrolla lo que él llama una taxonomía, que a primera vista parece casi como un mapa de navegación. Allí clasifica las amenazas a la privacidad en cuatro grandes categorías: recopilación, procesamiento, difusión e invasión. Dentro de cada una aparece un conjunto de actividades que permiten comprender dónde se generan los daños. En la categoría de recopilación, por ejemplo, ubica la vigilancia y el interrogatorio. La vigilancia no es solo la cámara instalada en un parque; puede ser también el rastreo constante de ubicación que hacen los celulares. En el interrogatorio incluye presiones para revelar datos que no siempre son necesarios. El problema radica en que ese tipo de cosas pasan desapercibidas porque las personas muchas veces se acostumbran a ceder información sin preguntarse para qué.

Después aparece el procesamiento, donde ubica la agregación, identificación, inseguridad y exclusión. Aquí es donde su teoría se vuelve más útil para contextos como el nuestro. La agregación, que es combinar datos dispersos para obtener un perfil más completo, es algo que hacen tanto entidades públicas como empresas. Por ejemplo, una EPS, un banco y una plataforma digital pueden tener cada una una parte de nuestra vida, y si llegan a juntarse, la imagen resultante es sorprendentemente íntima. La identificación se refiere a asociar información anónima con una persona, lo cual en países con sistemas débiles de seguridad informática se vuelve un riesgo frecuente. La inseguridad es básicamente la falta de protección técnica: bases de datos desactualizadas, sistemas vulnerables, empleados sin formación en manejo de datos. Y la exclusión, que Solove resalta mucho, ocurre cuando las personas no pueden acceder ni corregir la información que otros tienen sobre ellas. En Colombia es común que la gente ni siquiera sepa qué datos circulan en Datacrédito o en bases del Estado.

La tercera categoría, la difusión, comprende prácticas como la divulgación no autorizada, la exposición, la distorsión, el uso secundario y la violación de confidencialidad. Solove explica que no siempre el daño es que "se filtró un dato". A veces el daño está en cómo se presenta la información, porque una distorsión puede cambiar la reputación de alguien sin que los hechos sean falsos por completo. El uso secundario, que es usar datos para fines distintos al que fueron recolectados, en Colombia ocurre con frecuencia: los ciudadanos entregan datos para un trámite y después reciben llamadas de publicidad o se enteran de que la información terminó usada para un cruce de datos del que nunca fueron informados.

Solove termina con la categoría de la invasión, donde incluye prácticas como la interferencia en la vida privada y el acceso no autorizado a espacios personales, físicos o digitales. Esta es la parte más intuitiva porque se parece a la concepción clásica de privacidad que todos entendemos, pero Solove insiste en que es apenas una pieza del problema, no el centro como muchos creen.

Lo valioso del enfoque de Solove es que no mezcla estos daños; los diferencia para que sea más fácil analizarlos legalmente. En el fondo, podemos afirmar que la privacidad no es un ideal romántico, sino un conjunto de riesgos concretos que deben enfrentarse con herramientas jurídicas específicas. Su análisis ayuda incluso a evaluar decisiones judiciales: cuando un juez no entiende qué tipo de afectación se produjo, termina resolviendo el caso con criterios vagos o muy generalizados. En América Latina, donde las discusiones sobre privacidad suelen quedarse en afirmaciones generales sobre "la reserva de la información", su taxonomía permite poner orden y entender que detrás de cada violación hay un mecanismo claro.

Por otra parte, Helen Nissenbaum (2004) agrega otra capa cuando habla de la "integridad contextual". Su idea, que en palabras simples es que la privacidad depende de las expectativas del contexto social, explica por qué prácticas que parecen normales, como compartir datos entre entidades públicas o privadas, pueden volverse problemáticas si rompen esas expectativas. Al contrastar estas teorías con la realidad actual colombiana, observamos que su planteamiento no dista mucho de lo que los avances tecnológicos han acarreado en materia de privacidad y protección de la intimidad, muchas instituciones toman información

para fines distintos a los que los ciudadanos esperarían, lo que se traduce en afectación de confianza y uso indebido de estos datos.

De otro lado, trabajos como el de Martínez de Aguirre (2024) señalan que temas como la vigilancia también ha permeado la privacidad y ya no es algo excepcional sino incorporado en la estructura económica y estatal. En Colombia eso se refleja, por ejemplo, en el uso extendido de cámaras de seguridad, en la cooperación de datos entre entidades o en la dependencia de plataformas privadas que manejan enormes cantidades de información sin que exista claridad real sobre sus algoritmos. En Colombia, contamos con dos referentes normativos enfocados en la protección de la intimidad y los datos personales, estas son la Ley 1581 de 2012 y la Ley 1266 de 2008. La primera reconoce que la información personal pertenece a la esfera privada del individuo y que su manejo debe pasar por el consentimiento libre, lo que coincide con las concepciones modernas del derecho a la intimidad como autonomía. Sin embargo, la práctica muestra lo que autores como Solove advierten y es que el consentimiento no basta cuando el ciudadano enfrenta sistemas complejos de vigilancia o análisis automatizado cuyo funcionamiento no termina de comprender.

Por su parte, la Ley 1266, aunque más antigua y pensada para el ámbito financiero, introduce un aspecto importante: que la información económica también forma parte de la intimidad y puede afectar la dignidad de la persona. Esta visión coincide con los análisis doctrinales que destacan que la intimidad no se limita a lo corporal o familiar, sino que se extiende a los datos que generan perfiles, reputación y valor social, hoy profundamente arraigado a lo que se encuentra en perfiles digitales.

Ahora bien, a pesar de que la Ley 1581 de 2012 y la Ley 1266 de 2008 intentan construir un marco normativo para proteger la intimidad a través del control del uso de los datos, en la práctica, es otra la historia ya que el alcance de esas normas se ve limitado por las capacidades reales del Estado, por ejemplo, la Superintendencia de Industria y Comercio, que es la entidad encargada de vigilar el cumplimiento de estas leyes, tiene funciones amplias de control, sanción y orientación, pero estas funciones tienen dificultades técnicas y de recursos que hacen difícil que el sistema funcione como debería. Esto se nota en la cantidad de investigaciones que puede adelantar frente al tamaño del ecosistema digital y la velocidad con la que crecen las bases de datos. Incluso pareciera que, en ciertos sectores, existe una especie de normalización de la recolección desproporcionada de información personal, como si fuera un precio inevitable que debemos pagar por participar en la vida digital moderna. Esa normalización, que pasa casi desapercibida, debilita el espíritu de las leyes porque, aunque garantizan derechos en el papel, la vigilancia y la acumulación de datos se siguen expandiendo más rápido que los mecanismos efectivos de control estatal.

Sin embargo, este problema no es solo local, según el informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2021), los Estados deben establecer mecanismos de supervisión independientes con verdadera capacidad de rendición de cuentas para garantizar que las prácticas de recolección de datos no vulneren los principios de legalidad, necesidad y proporcionalidad. Además, la ONU advierte que, si la vigilancia estatal crece sin contrapesos, puede dañar otros derechos fundamentales como la libertad de expresión o de asociación, algo que resulta particularmente preocupante en sociedades donde la digitalización está avanzando sin control efectivo.

La Sentencia T-144 de 2024 de la Corte Constitucional pone en evidencia una dimensión práctica de este problema: esta es un ejemplo reciente que permite ver cómo la intimidad y el habeas data siguen siendo derechos frágiles en la práctica cotidiana, incluso cuando existen normas claras. En este caso, la Corte Constitucional estudió la instalación de cámaras de videovigilancia en un espacio terapéutico donde asistía un menor con autismo. La IPS, junto con la Secretaría Distrital de Salud, había implementado un sistema de grabación sin un consentimiento realmente libre e informado por parte de la madre, lo que terminó vulnerando no solo la intimidad del niño, sino también sus derechos a la salud y a la protección especial que la Constitución exige para personas en condición de vulnerabilidad.

Lo que resalta del fallo es que la Corte recordó algo básico, pero que a veces se olvida y es que la esencia del derecho a la intimidad está en el poder de control que cada persona tiene sobre su información. Esto implica que nadie puede ser sometido a vigilancia, registro o tratamiento de datos sin que existan salvaguardas claras, sin información suficiente y sin una justificación que sea proporcional. El problema, según lo que interpreta la Corte, no es la existencia de tecnología, sino la manera en que se usa sin considerar los efectos que tiene en la dignidad humana, especialmente cuando se trata de menores.

Además, la Corte insiste en que estas prácticas, que a primera vista parecen inofensivas o rutinarias, deben analizarse con cuidado porque la vigilancia no solo afecta la privacidad en un sentido estricto, sino que también condiciona la forma en que las personas se desenvuelven, se expresan y reciben servicios esenciales. El fallo subraya que la videovigilancia no puede naturalizarse como parte automática del funcionamiento institucional, pues su impacto va más allá del registro visual ya que puede producir temor, incomodidad y, en ciertos casos, incluso podría llegar a reforzar dinámicas de desigualdad.

El pronunciamiento de la Corte reafirma que la protección de datos no es un trámite formal ni algo que se resuelve con una simple firma, que como es bien sabido casi nadie lee todos los términos o peor aún, casi nadie los entiende a cabalidad. Es por ello que se requieren procesos claros, información transparente, consentimiento real y mecanismos de revisión. Y además muestra que, en el entorno digital actual, el riesgo

no proviene solamente de grandes plataformas, sino también de instituciones públicas o privadas que, a veces por desconocimiento o por costumbre, tratan la información personal como si fuera un elemento neutro que puede manipularse sin mayor reflexión.

Por otra parte, un elemento importante al revisar el impacto social del uso indebido o excesivo de datos es que no recae de igual manera sobre todas las personas. Los grupos vulnerables tales como jóvenes, comunidades rurales, mujeres en riesgo, migrantes, suelen quedar más expuestos porque tienen menos posibilidades de cuestionar o supervisar quién manipula su información. Diversas investigaciones sociales y jurídicas, varias de ellas recopiladas por el Observatorio de Derechos Humanos de la UFPSO, muestran que la protección de datos tiene efectos directos en el ejercicio de otros derechos como la libertad de expresión, el acceso a la justicia o la participación ciudadana. Una sociedad donde la vigilancia es constante tiende a generar autocensura, temor y desigualdad en el ejercicio de libertades.

Al respecto, Chilano (2023), advierte que el derecho a la intimidad, aunque reconocido constitucionalmente, se ve amenazado en la era digital porque los límites entre lo público y lo privado se difuminan, y especialmente los jóvenes tienden a aceptar como normales la exposición de datos personales. Esta tendencia cultural contribuye a lo que en Colombia se observa como una 'normalización' de la recolección masiva de información, en ese caso, si muchos usuarios participan sin percibir riesgo, las plataformas y entidades estatales encuentran menor resistencia. En ese sentido, la regulación normativa (como la Ley 1581 de 2012 o la Ley 1266 de 2008) choca no solo con la velocidad tecnológica, sino con la transformación de la conducta social.

Además de ello, en su obra también subraya que los marcos jurídicos clásicos deben adaptarse a estos nuevos escenarios tecnológicos. En Colombia, esta adaptación exige que las instituciones de supervisión no solo cumplan su función normativa, sino que también promuevan educación digital que incluya conciencia de riesgos y mecanismos de participación para que los ciudadanos reconozcan que el consentimiento o la exposición voluntaria no equivalen necesariamente a una protección real de su intimidad.

Esta perspectiva concuerda con lo propuesto por Moreno Hernández, Arias Moreno y Arias Moreno (2023) quienes señalan que en Colombia las redes sociales, en la que la mayoría de los usuarios son jóvenes, representan uno de los frentes más desafiantes para la protección de la intimidad. Para ellos, la exposición constante en plataformas digitales por medio de publicación de estados, interacciones, ubicación, y demás, erosiona la noción tradicional de un espacio privado, pues muchos usuarios ven el compartir sus datos como algo normal y cotidiano. Esa percepción cultural, especialmente entre los jóvenes, debilita la conciencia de riesgo y facilita la recolección masiva de información.

El estudio también critica que el régimen normativo vigente (Ley 1581 de 2012 y sus decretos) no se adapta completamente a las nuevas dinámicas de tratamiento de datos en redes sociales. Específicamente, identifican vacíos en regulaciones que podrían abordar el perfilamiento por algoritmos, la transferencia de datos entre plataformas y el análisis automatizado. Esta insuficiencia normativa se traduce en menores salvaguardas reales para los titulares, ya que no basta con tener derechos de acceso o rectificación si los mecanismos para ejercerlos son poco visibles, complejos o poco conocidos.

Como propuesta, los autores sugieren reforzar mecanismos de participación y control: en primer lugar, mediante educación digital para que los usuarios reconozcan sus derechos y riesgos; en segundo, a través de procesos más claros y accesibles para hacer valer derechos como la supresión de datos; y en tercero, exigiendo a las redes sociales una mayor transparencia y responsabilidad en su tratamiento de datos. Esto refuerza nuestra tesis central: no solo se trata de crear normas, sino de construir una cultura de protección de la intimidad que actúe como contrapeso a la lógica de vigilancia y participación digital.

Conclusión

A pesar de que Colombia ha dado pasos normativos relevantes, sin duda, todavía falta integrar un enfoque más práctico que combine educación digital, supervisión técnica, participación ciudadana y transparencia algorítmica. No basta con leyes generales y de contenido vago si las tecnologías evolucionan más rápido que las sanciones. Es necesario que las instituciones públicas adopten enfoques de privacidad por diseño, como lo propuesto por la Agencia Española de Protección de Datos (2019) y que las empresas tecnológicas que operan en el país justifiquen sus mecanismos de tratamiento de datos con evaluaciones claras y accesibles para los usuarios. La cooperación internacional puede ser útil, pero debe hacerse bajo principios de derechos humanos, como lo recomiendan organismos como la Oficina del Alto Comisionado de la ONU y los lineamientos de la OEA sobre protección de datos. Finalmente es necesario un cambio cultural en el que la ciudadanía vea la privacidad no como un obstáculo sino como condición para ejercer libertad y autonomía que debe ser plenamente garantizado.

Referencias

Agencia Española de Protección de Datos. (2019). Guía de Privacidad desde el diseño. https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf
Chilano, M. (2024). Intimidad en la era digital: análisis jurídico y enfoque juvenil sobre percepciones y prácticas. Derecom. Revista Internacional de Derecho de la Comunicación y de las Nuevas Tecnologías, 35, 41-57. https://revistas.ucm.es/index.php/DERE/article/view/98693
Congreso de al República de Colombia. (17 de octubre 2012). Ley de Protección de Datos Personales. [Ley 1581 de 2012] DO 48.587
Congreso de la República de Colombia. (31 de diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Ley 1266 de 2008] DO: 47219
Corte Constitucional de Colombia. (30 de abril de 2024). Sentencia T-144 de 2024. [M.P. CRISTINA PARDO SCHLESINGER]
Martinez, C. (2024). El Derecho a la Intimidad Revisitado. https://revista-aji.com/wp-content/uploads/2024/02/AJI20_Art_02.pdf
Moreno, C. Arias, A. Arias, I. (2023). Análisis del derecho a la intimidad en el contexto de la era digital en colombia: retos y oportunidades en la protección de la privacidad en redes sociales. https://repositorio.uniremington.edu.co/server/api/core/bitstreams/c1ca4fcd-5e79-4472-8e30-b587fc21e4f9/content
Naciones Unidas para los Derechos Humanos. (2021). A/HRC/60/45: El derecho a la privacidad en la era digital - Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. https://www.ohchr.org/es/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high
Nissenbaum, H. (2004). Privacy as Contextual Integrity. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr
Solove, D. (2006). A Taxonomy Of Privacy. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1376&context=penn_law_review
Reyes Quintero, D. D.., Lobo Contreras, M. R.., & Amaya Barbosa, L. D.. (2023). Derecho a la intimidad, Big Data y protección de datos: nuevos desafíos del ordenamiento jurídico colombiano. Postulados: Revista Sociojurídica, 1(1), 24–29.https://doi.org/10.22463/29816866.4256
López Rincón, G. A., & Quintero Sánchez, L. M. (2025). Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia. Postulados: Revista Sociojurídica, 2(2), 57–71. https://doi.org/10.22463/29816866.4300