EFICACIA DEL HABEAS DATA COMO REGULADOR DEL USO DE DATOS PERSONALES EN COLOMBIA: ¿GARANTÍA REAL O RETÓRICA LEGAL?*

María Catalina Jiménez Pascuales[1]
Miguel José Álvarez Pascuales[2]
Fernando José Marimon Casseres[3]
Luis Jair de Avila Anaya[4]

1. Introducción

En la época actual, los datos personales han convertido en parte de la vida diaria de cada individuo. En este contexto, la circulación de información es el motor de la economía digital; sin embargo, esta fluidez plantea un dilema ético profundo sobre el control de nuestra propia esencia.

Aunque el derecho al Habeas Data cuenta con una trayectoria sólida en Colombia, su propósito ha experimentado una evolución fascinante. Lo que nació como una herramienta para gestionar la información crediticia se ha transformado hoy es un elemento fundamental. No obstante, nos enfrentamos a una realidad desafiante: en un entorno donde las filtraciones y el acceso no autorizado parecen haberse normalizado, cabe preguntarnos si la Ley 1581 de 2012 conserva su eficacia real.

Este artículo sostiene con convicción que la efectividad de la norma no se ve limitada por la tecnología en sí misma, sino por tres factores críticos que debemos abordar con urgencia: las marcadas disparidades tecnológicas entre regiones, las vulnerabilidades inherentes al factor humano y las limitaciones estructurales de nuestros organismos reguladores. El problema, por tanto, trasciende lo técnico para situarse en el plano de lo humano. Al final del camino, proteger el dato es proteger la privacidad y la dignidad de cada ciudadano, un reto que, aunque complejo, representa la oportunidad de construir una sociedad digital más justa y resiliente.

2. Contexto Normativo

Para dimensionar el elemento perjudicial, es necesario retroceder y reconocer el camino de empoderamiento que Colombia ha recorrido. El punto de inflexión se halla en la Constitución Política de 1991, específicamente en su Artículo 15. Este no fue un sim-

* Este artículo de opinión se elabora como parte del proceso académico de la asignatura de Investigación, en el marco del Programa de Especialización en Derecho Procesal de la Universidad Libre.

1 Abogada, Estudiante de la Especialización en Derecho Procesal de la Universidad Libre, Seccional Cartagena. Autor de correspondencia: mariacatalinaj21@hotmail.com
2 Abogado, Estudiante de la Especialización en Derecho Procesal de la Universidad Libre, Seccional Cartagena
3 Abogado, Estudiante de la Especialización en Derecho Procesal de la Universidad Libre, Seccional Cartagena
4 Abogado, Estudiante de la Especialización en Derecho Procesal de la Universidad Libre, Seccional Cartagena

ple cambio de palabras; fue una revolución jurídica que nos otorgó una nueva lente para proteger nuestra esfera privada en un mundo que empezaba a interconectarse.

A partir de este hito, la Corte Constitucional ha desempeñado un papel importante. A través de su jurisprudencia, el derecho a la protección de datos dejó de ser una sombra de otros derechos para ser reconocido como un derecho fundamental autónomo. Este avance nos sacó de la visión clásica y limitada de la "intimidad" para llevarnos hacia la autodeterminación informativa: el poder soberano que tiene cada individuo de decidir qué se hace con su información. Comprender esta transición no solo es un ejercicio académico; es reconocer que tenemos en nuestras manos una herramienta poderosa para defender nuestra identidad frente a las estructuras de poder digital.

2.1. Entrada en vigencia de la Ley 1581 de 2012

La llegada de la Ley 1581 no fue un simple trámite legislativo; fue la respuesta necesaria a una ciudadanía que reclamaba protección en su vida cotidiana. Esta norma estableció los pilares fundamentales que hoy nos sostienen: legalidad, libertad, transparencia y, sobre todo, la confidencialidad. Este último principio es un compromiso sagrado: exige que quienes custodian nuestra información aseguren su reserva absoluta, incluso cuando el vínculo comercial o administrativo ha finalizado.

Es cierto que esta ley se diseñó bajo un ideal de orden que la realidad digital, con su ritmo frenético, a menudo desafía. Muchas organizaciones han optado por una "adhesión técnica" —cumpliendo apenas con lo mínimo para evitar sanciones— sin adoptar una verdadera cultura de protección. Sin embargo, lejos de ser una derrota, este escenario es una invitación al liderazgo ético.

Contamos con una base sólida; el marco definitorio es robusto y claro. El desafío actual es transformar ese cumplimiento mecánico en medidas reales y profundas que pongan al ser humano en el centro. Estamos en el momento perfecto para pasar de la norma escrita a la protección vivida, asegurando que la tecnología sea siempre un aliado de nuestra privacidad y nunca una amenaza para nuestra integridad.

3. Riesgos y Vulnerabilidades en el entorno Digital

Hoy más que nunca, la confidencialidad se encuentra en una encrucijada donde las fronteras físicas se han desvanecido. Ya no basta con proteger los archivos bajo llave o restringir el acceso a un recinto; los riesgos han evolucionado hacia un ecosistema digital donde los peligros crecen a un ritmo exponencial, desafiando constantemente nuestras capacidades de gestión. No obstante, reconocer esta complejidad no debe ser motivo de desánimo, sino el motor que nos impulse a fortalecer nuestras defensas.

La sofisticación de estas amenazas nos exige dejar atrás la visión reactiva y avanzar hacia una cultura de prevención inteligente. En este entorno digital tan vasto como complejo, la vulnerabilidad no es una sentencia, sino una oportunidad para innovar en nuestros protocolos de seguridad. Estamos en una etapa histórica donde la tecnología, si bien presenta desafíos, también nos brinda las herramientas más potentes jamás creadas para salvaguardar lo más valioso que poseemos: nuestra integridad informativa. Superar este reto es posible si unimos la robustez técnica con una voluntad inquebrantable de proteger la privacidad ciudadana.

3.1. Amenazas cibernéticas y el avance del delincuencia a través del hackeo

En la actualidad, el aumento en la sofisticación de ataques como el *phishing* y el *malware* ha puesto a prueba la solidez de las bases de datos en Colombia, revelando grietas que exigen nuestra atención inmediata. Sin embargo, más allá de la infraestructura técnica, debemos comprender que una filtración de datos no es solo un fallo de seguridad; es un evento que impacta la esfera más íntima de miles de ciudadanos. Cuando nombres y documentos de identidad quedan expuestos, lo que está en juego no es solo la reputación de una entidad, sino la tranquilidad y la seguridad de las personas detrás de esos registros.

Aunque estos incidentes suelen ser ampliamente publicitados y generar un clima de incertidumbre, es fundamental ver este escenario como un punto de inflexión hacia la excelencia. Estas debilidades no son obstáculos insuperables, sino señales claras de que debemos fortalecer nuestra cultura digital. Tenemos la oportunidad de transformar estos desafíos en experiencias de aprendizaje que nos permitan robustecer nuestros sistemas. Al proteger cada dato, estamos blindando la vida y la confianza de los colombianos. La seguridad total puede ser un ideal complejo, pero cada paso que damos hacia la protección proactiva es una victoria ganada para la privacidad y un paso firme hacia una sociedad digital más resiliente y humana.

4. La Brecha Regional: El desafío y la promesa de Bolívar

Un análisis riguroso de la eficacia normativa nos obliga a mirar más allá de los centros administrativos del país y reconocer las asimetrías que persisten en nuestro territorio. El contraste entre la implementación de la Ley 1581 en las grandes metrópolis frente a las realidades de Cartagena y las zonas periféricas de Bolívar es notable. Mientras las capitales han logrado consolidar robustas estructuras de protección, las regiones enfrentan desafíos únicos que exigen una atención diferenciada.

Sin embargo, esta disparidad no debe verse como un destino, sino como una oportunidad histórica para la equidad. Cerrar esta brecha es el camino para garantizar que el de-

recho a la privacidad no sea un privilegio de unos pocos, sino una realidad palpable para cada ciudadano bolivarense. Al fortalecer las capacidades tecnológicas y el conocimiento normativo en nuestra región, no solo estamos corrigiendo una desigualdad técnica, sino que estamos reivindicando la soberanía digital de nuestras comunidades. Bolívar tiene el potencial de convertirse en un modelo de resiliencia, demostrando que, con voluntad y una visión inclusiva, es posible proteger la dignidad humana con la misma firmeza en la ciudad como en la provincia.

4.1. Institucionalidad y PYMES: Hacia una ética de la confianza

En el tejido empresarial de Cartagena, las pequeñas y medianas empresas (PYMES) se encuentran en un momento decisivo. Actualmente, muchas de ellas perciben la protección de datos como un mero trámite administrativo o una carga burocrática, dejando en un segundo plano la esencia del deber ético y legal que esta implica. Esta visión suele acentuarse cuando el despliegue de nuevas plataformas digitales no cuenta con un acompañamiento institucional sólido que brinde seguridad a los emprendedores.

Sin embargo, este escenario representa una oportunidad de oro para diferenciarse. El cumplimiento de la Ley 1581 no debe verse como un obstáculo, sino como el mayor activo de confianza que una empresa puede ofrecer a sus clientes. Al integrar la privacidad como un valor central, nuestras PYMES en Cartagena no solo cumplen la norma, sino que se convierten en referentes de integridad y competitividad en el mercado global. Es hora de liderar una transición donde la tecnología y la ética caminen de la mano, impulsadas por un respaldo institucional que empodere el talento local.

4.2. Riesgo en los servicios públicos.

La digitalización de los servicios públicos ha generado un gran avance en el acceso a la información; no obstante, este avance ha generado un flujo de datos sin precedentes que nuestra infraestructura tecnológica aún lucha por gestionar con total seguridad. Es cierto que la falta de herramientas robustas ha expuesto a los ciudadanos a escenarios de vulnerabilidad, pero reconocer esta realidad es el primer paso hacia una reconstrucción tecnológica necesaria y urgente.

Más que una señal de alarma, este riesgo extremo debe ser el catalizador para una inversión estratégica en resiliencia digital. Tenemos ante nosotros el desafío de blindar los servicios esenciales, asegurando que cada ciudadano pueda interactuar con el Estado con la absoluta certeza de que su información está protegida. Al fortalecer nuestra infraestructura, no solo cerramos brechas de

9 Corte Constitucional, 2004. Sentencia T-983A/04.
10 Corte Constitucional, 2004. Sentencia T-983A/04.

seguridad, sino que construimos un puente de confianza indestructible entre la administración pública y la comunidad. El futuro de los servicios en Bolívar es digital, y está en nuestras manos asegurar que sea, ante todo, un futuro seguro y digno.

5. La eficacia de la protección de los datos personales.

El sistema de protección de datos en Colombia se encuentra en una etapa de madurez necesaria. Actualmente, contamos con herramientas valiosas como las quejas ante la Superintendencia de Industria y Comercio (SIC) y la acción de tutela; sin embargo, estos mecanismos han operado bajo una lógica mayoritariamente reactiva: actúan una vez que el daño ya ha ocurrido. Este panorama no debe desmotivarnos, sino invitarnos a evolucionar hacia un modelo donde la prevención sea nuestra mejor defensa.

5.1. El Rol de la SIC: Más allá de la Sanción

Es innegable el esfuerzo titánico que la SIC ha realizado mediante su labor sancionadora, sentando precedentes importantes en el país. No obstante, el verdadero éxito de la regulación no reside en la cuantía de las multas, sino en la capacidad de evitar que las vulneraciones sucedan. En contextos donde el conocimiento de la norma es limitado, la labor de la Superintendencia tiene el potencial de transformarse: de ser un ente puramente correctivo para convertirse en un faro de educación y acompañamiento. Al iluminar el camino de las organizaciones con pedagogía, la SIC puede sembrar una cultura de cumplimiento que florezca incluso en las regiones más apartadas.

5.2. El Principio de Responsabilidad Demostrada

Para que la privacidad deje de ser una aspiración y se convierta en una realidad, debemos abrazar con entusiasmo el principio de Responsabilidad Demostrada (*Accountability*). Este no es un concepto abstracto; es una invitación a la excelencia operativa. Se trata de integrar auditorías, controles verificables y medidas integrales en la rutina diaria de cada institución, ya sea pública o privada.

Implementar estas acciones no debe verse como una carga, sino como la construcción de un sello de confianza y calidad. Cuando el procesamiento de datos se gestiona con transparencia y rigor, las organizaciones no solo evitan riesgos, sino que elevan su valor ante la sociedad. Estamos ante la oportunidad de liderar un cambio donde la protección de la información sea parte del ADN institucional. El camino hacia una Colombia digitalmente segura es ambicioso, pero con cada medida verificable que tomamos, estamos asegurando un futuro donde la tecnología y la libertad caminen siempre de la mano.

6. Conclusión

La protección de datos personales no debe entenderse simplemente como el cumplimiento de una norma técnica; debe asumirse como un compromiso moral, legal y social ineludible. Estamos ante una oportunidad histórica para trascender el papel y convertir el derecho al *Habeas Data* —que por años ha sido una valiosa promesa constitucional— en una garantía funcional y tangible para cada habitante del país, sin importar su ubicación geográfica.

Al fortalecer nuestra infraestructura, educar el factor humano y abrazar la responsabilidad demostrada, estamos haciendo mucho más que blindar bases de datos: estamos protegiendo la dignidad humana básica de cada ciudadano. El camino hacia la excelencia digital en Colombia, y específicamente en regiones con grandes retos como Bolívar, es una invitación a construir un futuro donde la tecnología sea un espacio de seguridad y respeto. Asegurar la información es, en última instancia, asegurar nuestra libertad. Si logramos este compromiso colectivo, no solo cumpliremos con la ley, sino que estaremos cimentando una sociedad digital más justa, humana y profundamente resiliente.

Referencias

Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*.

Constitución Política de Colombia. (1991). *Gaceta Constitucional No. 116*.

Corte Constitucional de Colombia. (1992, 16 de junio). *Sentencia T-414/92* (Ciro Angarita Barón, M. P.).

Corte Constitucional de Colombia. (2021, 13 de mayo). *Sentencia SU-139/21* (Jorge Enrique Ibáñez Najar, M. P.).