ANÁLISIS CRÍTICO DEL MARCO LEGAL QUE RODEA LA PRIVACIDAD DE LOS DATOS

Andrea Carolina Herrera Esparragoza[1]
Mariana Segovia Acevedo[2]

INTRODUCCIÓN

La privacidad de los datos, hoy por hoy, se ha consolidado como una de las preocupaciones más acuciantes en la sociedad contemporánea, en un contexto donde la recopilación, almacenamiento y uso de información personal se han intensificado exponencialmente debido a los diversos avances tecnológicos. Este fenómeno ha puesto en tela de juicio la efectividad del marco legal vigente, cuestionando su capacidad para salvaguardar los derechos individuales frente a las múltiples amenazas que emergen en un entorno digital cada vez más intrincado y dinámico.

Este artículo se propone realizar un análisis crítico y profundo del régimen jurídico actual en materia de privacidad de datos, evaluando no solo su suficiencia y adecuación, sino también su implementación práctica y su capacidad de adaptación a las innovaciones tecnológicas. Al hacerlo, se busca arrojar luz sobre las áreas que requieren reforma o mejora, con el fin de garantizar una protección efectiva y robusta de los datos personales en esta era digital.

PREGUNTA PROBLEMA

¿En qué medida las leyes actuales de privacidad de datos garantizan la protección efectiva de los derechos individuales frente a los riesgos emergentes de la recopilación, almacenamiento y uso de datos personales en la era digital?

DESARROLLO

Análisis de la legislación relevante en cuanto a privacidad de datos

Para comprender la efectividad y los desafíos del marco legal colombiano en materia de privacidad de datos, es esencial examinar algunas de las normativas más relevantes que constituyen la base de esta protección. A continuación, se analizan tres leyes fundamentales y disposiciones del Código Penal que regulan la gestión y protección de los datos personales en Colombia: ***I)*** *la Ley Estatutaria 1266 de 2008,* ***II)*** *la Ley Estatutaria 1581 de 2012,* ***III)*** *la Ley 594 de 2000 y* ***VI)*** *el Título VII BIS del Código Penal*.

1 Estudiante de Derecho, Universidad Libre – Seccional Cartagena de Indias: andreac-herrerae@unilibre.edu.co
2 Estudiante de Derecho, Universidad Libre – Seccional Cartagena de Indias: mariana-segoviaa@unilibre.edu.co

Cada una de estas normativas aborda aspectos cruciales para la protección de la información, estableciendo derechos, obligaciones y sanciones que buscan garantizar la privacidad y seguridad de los datos en un contexto tecnológico en constante evolución.

Ley Estatutaria 1266 de 2008

La **Ley Estatutaria 1266 de 2008**, también conocida como la *"Ley de Habeas Data"*, se constituye como un pilar fundamental en la regulación del manejo de la información contenida en bases de datos personales en Colombia. Esta ley se enfoca especialmente en los sectores financieros, crediticios, comerciales y de servicios, donde el manejo de datos sensibles es una práctica común y necesaria para el funcionamiento de las actividades económicas.

Uno de los aspectos más relevantes de esta ley es que establece disposiciones generales para la protección de datos personales, permitiendo que las entidades que recolectan y administran esta información lo hagan bajo estrictas normas de seguridad y confidencialidad. La ley busca asegurar que los datos sean utilizados de manera responsable y únicamente para los fines autorizados por el titular de la información.

La Ley 1266 de 2008 también establece el derecho de los ciudadanos a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bases de datos personales. Este derecho es crucial, ya que permite a los individuos tener control sobre su información personal y corregir cualquier inexactitud que pueda afectar su reputación o su situación financiera. Además, la ley impone obligaciones a las entidades responsables de las bases de datos, exigiéndoles adoptar medidas técnicas, humanas y administrativas para garantizar la seguridad de los datos y prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado.

Un aspecto crítico de esta ley es la introducción del concepto de Habeas Data, que otorga a las personas la facultad de solicitar información sobre los datos que se han recogido sobre ellas y cómo se están utilizando. Este mecanismo legal fortalece la protección de la privacidad y permite a los ciudadanos defenderse contra el uso indebido de su información personal. La implementación de esta ley ha tenido un impacto significativo en la regulación de la privacidad de los datos en Colombia, aunque su aplicación práctica ha revelado desafíos y áreas de mejora que aún deben ser abordadas.

Ley Estatutaria 1581 de 2012

La Ley Estatutaria 1581 de 2012, conocida como la Ley de Protección de Datos Personales, se promulga con el objetivo de desarrollar el derecho constitucional de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. Esta ley es

esencial para la protección de la privacidad de los datos personales y busca armonizar la legislación colombiana con los estándares internacionales en materia de protección de datos.

Esta ley establece un marco normativo integral que regula la recolección, almacenamiento, uso, circulación y supresión de datos personales, garantizando que estos procesos se realicen con el consentimiento previo, expreso e informado del titular de los datos. Además, la ley impone responsabilidades claras a los responsables del tratamiento de datos, obligándolos a implementar medidas adecuadas para proteger la información contra riesgos como la pérdida, el acceso no autorizado o el uso fraudulento.

Esta ley también crea la figura del *"Delegado de Protección de Datos"*, encargado de velar por el eficaz cumplimiento de las normas de protección de datos dentro de las organizaciones.

Esta figura es clave para asegurar que las empresas y entidades públicas adopten políticas de privacidad adecuadas y respondan de manera efectiva a las solicitudes y reclamaciones de los titulares de datos.

Adicionalmente, la ley establece sanciones para las entidades que incumplan sus disposiciones, incluyendo multas significativas y la posibilidad de que se ordene la suspensión de las actividades relacionadas con el tratamiento de datos personales. Estas sanciones tienen un efecto disuasorio importante y refuerzan la necesidad de cumplir con los estándares de protección de datos establecidos por la ley.

Ley 594 de 2000

La Ley 594 de 2000, conocida como la Ley General de Archivos, establece el marco normativo para la gestión documental en Colombia. Aunque su enfoque principal es la organización, conservación y manejo de los archivos, tiene implicaciones directas en la protección de la privacidad de los datos personales al regular cómo las entidades públicas y privadas deben tratar la información que producen y reciben en el ejercicio de sus funciones.

Parte de su esencialidad en el contexto que abordamos es que reconoce la importancia de los archivos como herramientas fundamentales para la gestión administrativa, económica, política y cultural del Estado. Esto incluye el manejo responsable de los datos contenidos en dichos archivos; así al regular la "función archivística", la ley establece que los servidores públicos son responsables del manejo adecuado de los documentos, lo que abarca la protección de datos personales y sensibles. La conservación y uso de documentos están sujetos a principios de racionalidad, modernización y responsabilidad, asegurando que se respeten los derechos de las personas en cuanto a la información contenida en dichos archivos.

2.1.3.1. Acceso y Control Ciudadano

Esta ley garantiza el acceso de los ciudadanos a los archivos públicos, salvo las excepciones establecidas jurisprudencial y constitucionalmente. En este sentido, la privacidad de los datos se protege mediante limitaciones específicas al acceso a información que puede comprometer la seguridad o los derechos fundamentales de las personas, como la privacidad. La normativa también hace referencia a los archivos privados de interés público, que pueden contener información personal protegida, subrayando la necesidad de equilibrar el acceso a la información con el derecho a la privacidad.

Así, el "Archivo General de la Nación", como órgano encargado de coordinar la función archivística, tiene el deber de orientar y supervisar el cumplimiento de estas disposiciones. La ley enfatiza la importancia de garantizar la integridad y autenticidad de los documentos, lo cual incluye medidas de seguridad para evitar el uso indebido de datos personales, promoviendo así una gestión archivística que respete los derechos de privacidad.

INVESTIGACIÓN JURISPRUDENCIAL Y DECISIONES REGULATORIAS

Sentencia C-1011 de 2008

Esta sentencia, como ejemplo perfecto de las implicaciones derivadas de la protección y privacidad de los datos personales, se refiere al control de constitucionalidad del proyecto de ley estatutaria sobre hábeas data y el manejo de información contenida en bases de datos personales. En esta sentencia, la Corte analizó tanto los aspectos formales del trámite legislativo como los materiales, en relación con la regulación del derecho al hábeas data. Uno de los principios fundamentales evaluados fue el de unidad de materia. La Corte sostuvo que la ley no puede incluir disposiciones que no guarden relación con el núcleo temático de la misma. En este caso, el proyecto de ley se enfocaba en la regulación del derecho al hábeas data, con énfasis en el ámbito financiero, crediticio, comercial y de servicios, lo que fue considerado adecuado dentro de los parámetros del principio de unidad de materia. Cada una de las disposiciones del proyecto tenía una conexión clara con la protección y administración de los datos personales.

La Corte también revisó el cumplimiento de los principios de consecutividad e identidad en el trámite legislativo. Aunque se realizaron modificaciones al proyecto de ley durante su paso por el Congreso, estas no fueron consideradas como cambios sustanciales o la introducción de temas nuevos. Las modificaciones, tales como la inclusión de la definición de agencia de información o normas sobre la caducidad de datos financieros, fueron vistas como ajustes necesarios y relacionados con el núcleo central de la ley.

Derecho al Hábeas Data

El proyecto de ley estableció un marco jurídico para la protección de datos personales en bases de datos financieras, crediticias y comerciales. Este derecho permite a los titulares de datos solicitar su inclusión, exclusión, corrección o actualización, además de limitar su divulgación. Sin embargo, la Corte aclaró que este marco regulaba solo una parte del derecho al hábeas data, enfocado en los datos financieros, y no abarcaba otros tipos de administración de datos personales.

Este proyecto previó ciertos ámbitos de exclusión de la aplicación de sus normas, como las bases de datos destinadas a la inteligencia del Estado y los registros públicos de las cámaras de comercio. La Corte consideró que estas exclusiones eran legítimas, dado que dichos datos tienen un propósito distinto al de los datos crediticios y financieros. Sin embargo, destacó que estos ámbitos excluidos no carecen de protección bajo el derecho fundamental al hábeas data.

Finalmente, la Corte revisó el artículo 20 del proyecto, que ordena al Gobierno ajustar las estructuras de las superintendencias responsables de la vigilancia y control del manejo de datos. La Corte concluyó que esta disposición no constituye un mandato imperativo de gasto público, sino una autorización para que el Gobierno adopte las medidas necesarias, respetando las normas presupuestales vigentes.

Decisiones regulatorias de la Superintendencia de Industria y Comercio (SIC)

La Superintendencia de Industria y Comercio (SIC) de Colombia, como ente regulador en materia de protección de datos personales, ha desempeñado un rol crucial en el desarrollo e implementación del marco normativo que protege la privacidad de los datos personales -más en esta era digital-. A través de sus decisiones, la SIC ha establecido lineamientos que garantizan el respeto por los derechos de los titulares de datos y promueven el cumplimiento de la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales.

En el contexto de la era digital, la SIC ha enfocado sus decisiones regulatorias en varios aspectos clave:

Consentimiento Informado	La SIC ha enfatizado que las empresas y entidades querecopilan datos personales deben obtener el consentimiento claro, previo e informado de los titulares. Las decisiones de la SIC subrayan la importancia de que este consentimiento no solo sea explícito, sino que también se brinde en condiciones que permitan al usuario comprender el alcance del tratamiento de sus datos, especialmente en entornos digitales donde los contratos y políticas de privacidad suelen ser complejos.

Principio de Finalidad	En sus resoluciones, la SIC ha reiterado que los datos personales solo pueden ser utilizados para los fines específicos para los cuales fueron recopilados. Las empresas que excedan estos límites o utilicen los datos para fines diferentes sin la autorización expresa del titular han sido sancionadas. Este principio se refuerza en la era digital, donde la recopilación masiva de datos puede derivar en el uso no autorizado o en la comercialización de la información.
Transferencia Internacional de Datos	La SIC ha sido clara en que cualquier transferencia de datos personales hacia países que no ofrezcan niveles adecuados de protección requiere la autorización del titular, de acuerdo con el principio de seguridad. En la era de la globalización digital, donde los datos pueden fluir muy fácilmente a través de fronteras, las decisiones de la SIC buscan asegurar que las empresas colombianas cumplan con los estándares internacionales en materia de protección de datos.
Seguridad de la Información	La SIC ha sancionado a empresas que no implementan medidas técnicas y administrativas adecuadas para proteger los datos personales de accesos no autorizados o de vulneraciones, como hackeos o filtraciones. En la era digital, donde los riesgos de ciberseguridad son elevados, la SIC ha insistido en la necesidad de que las organizaciones adopten protocolos de seguridad robustos, alineados con las mejores prácticas internacionales.
Derechos de los Titulares	A través de sus decisiones, la SIC ha garantizado el derecho de los titulares a acceder, actualizar, rectificar y eliminar sus datos personales. En particular, la SIC ha intervenido en casos donde las empresas dificultan el ejercicio de estos derechos, estableciendo sanciones para aquellas que no cumplan con los tiempos o procedimientos establecidos por la ley.
Tratamiento de Datos Sensibles	La SIC ha puesto un enfoque especial en el tratamiento de datos sensibles (como los relacionados con la salud, creencias religiosas o políticas, orientación sexual, entre otros), exigiendo un nivel de protección más alto. Las decisiones regulatorias han dejado claro que el manejo de estos datos requiere un consentimiento explícito y debe ser tratado con extremo cuidado.

Las decisiones de la SIC reflejan una preocupación constante por equilibrar el avance tecnológico con la protección de los derechos de privacidad de los ciudadanos. En la era digital, donde la recopilación y tratamiento de datos personales es más intensa y compleja, la SIC ha actuado para fortalecer el marco legal existente, ajustándose a los desafíos emergentes y protegiendo a los ciudadanos frente a posibles abusos en el uso de sus datos personales.

Las multas impuestas y los precedentes judiciales generados a partir de sus decisiones han contribuido a consolidar una cultura de protección de datos en Colombia, que busca

garantizar un equilibrio entre innovación digital y privacidad.

EVALUACIÓN DEL IMPACTO DE TECNOLOGÍAS EMERGENTES

Inteligencia Artificial (IA)

Pese a los intentos de la SIC y otras instituciones por salvaguardar el espectro que rodea a los datos personales, la irrupción de la Inteligencia Artificial (IA) terminó complicando -de manera revolucionaria- el tratamiento de los datos personales, transformando profundamente la manera en que las organizaciones recopilan, procesan y utilizan la información. Esta tecnología ha dado lugar a capacidades sin precedentes para analizar grandes volúmenes de datos (big data), identificar patrones ocultos y realizar predicciones precisas sobre comportamientos futuros, lo que ha impulsado avances significativos en sectores como la salud, el comercio, la seguridad y los servicios financieros. Sin embargo, el poder de la IA también ha introducido una nueva serie de desafíos para la privacidad y la protección de la información en el entorno digital, planteando preocupaciones sobre el control que los individuos tienen sobre sus propios datos y la posible vulneración de sus derechos fundamentales.

En este contexto, la capacidad de los sistemas de IA para procesar datos de forma automatizada y a gran escala ha dado lugar a un uso más sofisticado e intrusivo de los datos personales, lo que requiere un marco legal más robusto y actualizado. Las técnicas avanzadas de aprendizaje automático y de análisis predictivo, aunque útiles para mejorar la eficiencia y personalización de los servicios, también tienen el potencial de abusar de la información personal si no se implementan bajo estrictas salvaguardias. La recopilación de datos sin el consentimiento informado adecuado, la creación de perfiles detallados de los usuarios, o el uso de algoritmos que toman decisiones automatizadas sin la supervisión humana son solo algunos de los riesgos que han surgido en esta era digital, donde la IA juega un papel central.

Este panorama demanda una regulación efectiva y proactiva por parte de entidades como la Superintendencia de Industria y Comercio (SIC), cuya labor es fundamental para garantizar que el desarrollo y la implementación de la IA respeten los derechos de privacidad consagrados en la Constitución y en la legislación colombiana, como la Ley 1581 de 2012, que regula el tratamiento de datos personales. La SIC, en su papel de entidad supervisora y reguladora, enfrenta la tarea de equilibrar la promoción de la innovación y el crecimiento tecnológico con la protección de los derechos de los ciudadanos, estableciendo normas claras que limiten el uso excesivo de los datos personales y que aseguren la transparencia, la rendición de cuentas y el consentimiento informado en el uso de la IA. Este marco legal no solo debe estar preparado para regular el uso actual de la IA, sino que

también debe ser lo suficientemente flexible como para adaptarse a los avances futuros en la tecnología, previendo y mitigando posibles riesgos emergentes. La capacidad de la SIC para crear regulaciones dinámicas, promover buenas prácticas en la protección de datos y hacer cumplir las sanciones en casos de abuso será clave para preservar la confianza en la IA como una herramienta poderosa pero controlada en favor de la sociedad, y no en detrimento de los derechos individuales.

Ahora, todo esto recae en los diversos retos que recaen en la IA respecto a la privacidad de los datos:

0**Recopilación Masiva de Datos**	Los sistemas de IA requieren una gran cantidad de datos para funcionar de maneraeficiente. Estos datos provienen de diversasfuentes, incluyendo interacciones en redes sociales, aplicaciones móviles, búsquedas en Internet y dispositivos inteligentes. La recopilación masiva y automatizada de datos plantea interrogantes sobre el consentimiento informado y el control que los titulares tienen sobre su información. Eneste contexto, las regulaciones que garantizan la protección de los datos deben adaptarse para asegurar que la recopilación de información por parte de sistemas de IA se realice conforme a los principios de la Ley 1581 de 2012.
Predicción y Perfilamiento	La IA permite generar perfiles detallados sobre los usuarios, basándose en la información que estos generan. Estos perfiles pueden ser utilizados para segmentar a las personas según sus preferencias, hábitos de consumo, situación financiera, o incluso predicciones sobre su comportamiento futuro. Aunque esto puede ser útil para personalizar servicios o mejorar la experiencia del usuario, también genera riesgos en términos de discriminación, manipulación y violación de la privacidad, ya que las personas pueden ser clasificadas o excluidas sin su conocimiento ni consentimiento. Este riesgo exige un enfoque más riguroso en la protección de los datos personales, así como la actualización de las normativas para adaptarse a las nuevas capacidades tecnológicas.

Indiscutiblemente, la integración de la IA en el tratamiento de datos personales requiere una adaptación del marco regulatorio existente y una supervisión activa de las entidades regulatorias como la SIC. Si bien la IA ofrece grandes oportunidades para mejorar los servicios y optimizar procesos, también plantea riesgos significativos para la privacidad de las personas. Por ello, es esencial que se establezcan principios claros sobre el uso ético y responsable de la IA, protegiendo los derechos fundamentales de los titulares de los datos y asegurando que las decisiones tomadas por estos sistemas sean transparentes, equitativas y sujetas a supervisión humana cuando sea necesario.

OBSERVACIONES Y RECOMENDACIONES

Transparencia en el manejo de datos

Uno de los aspectos fundamentales para garantizar la confianza de los ciudadanos en el manejo de sus datos personales es la transparencia. En la actualidad, muchas empresas y entidades gubernamentales que recogen, almacenan y procesan datos personales no siempre comunican de manera clara y comprensible cómo se manejan estos datos. La falta de transparencia genera incertidumbre entre los usuarios, quienes muchas veces no saben con precisión qué tipo de información se está recopilando, para qué fines se utiliza y con quién se comparte.

Es crucial que las organizaciones adopten medidas que permitan a los usuarios tener acceso a información detallada y en lenguaje claro sobre el tratamiento de sus datos. Esto incluye una política de privacidad accesible, la notificación clara de cualquier cambio en el manejo de los datos y el uso de consentimientos informados para la recolección de información. La implementación de herramientas que permitan a los usuarios gestionar fácilmente su consentimiento y retirar el mismo en cualquier momento también debe ser una prioridad. Así mismo, es recomendable fomentar auditorías regulares e independientes sobre el cumplimiento de las normativas de protección de datos, que puedan ser consultadas por los usuarios.

Aplicación de sanciones

La regulación en materia de protección de datos personales debe estar respaldada por un sistema efectivo de sanciones para aquellas entidades que incumplan las normas establecidas. Si bien existen normativas vigentes, como la Ley 1581 de 2012 en Colombia, es esencial que las autoridades competentes, como la Superintendencia de Industria y Comercio (SIC), apliquen de manera rigurosa las sanciones correspondientes cuando se detecten infracciones. La implementación efectiva de sanciones no solo actúa como un disuasivo para el incumplimiento, sino que también refuerza la importancia de respetar los derechos de privacidad de los ciudadanos.

En este sentido, es recomendable que las sanciones incluyan no solo multas económicas proporcionales a la gravedad de la infracción, sino también medidas correctivas como la suspensión temporal o definitiva del tratamiento de datos. Además, las entidades sancionadas deberían estar obligadas a publicar de manera pública las infracciones cometidas y las medidas correctivas adoptadas para remediarlas. Esta transparencia contribuirá a generar confianza y actuará como una herramienta de rendición de cuentas.

Asimismo, es importante revisar periódicamente las sanciones establecidas en la normativa vigente para asegurar que estas sean acordes con la evolución tecnológica y con la magnitud de los riesgos que las nuevas tec-

nologías, como la Inteligencia Artificial y el Big Data, pueden representar para la privacidad de los datos personales. Las entidades reguladoras deben tener el poder de imponer sanciones ejemplares en casos de violaciones graves, así como de restringir temporalmente el acceso a la información en caso de sospechas de un manejo indebido de los datos.

CONCLUSIONES

En la era digital, la protección de los datos personales se ha convertido en un desafío central para las sociedades modernas. El incremento en la cantidad de datos generados, así como la capacidad de tecnologías avanzadas como la Inteligencia Artificial para procesarlos, ha transformado radicalmente el entorno regulatorio, exigiendo un enfoque más riguroso y adaptado a las nuevas realidades. La Superintendencia de Industria y Comercio (SIC), como ente encargado de velar por la protección de los datos en Colombia, juega un papel clave en garantizar que tanto las empresas como las entidades públicas cumplan con las normativas que protegen los derechos de los ciudadanos.

La necesidad de un marco legal robusto, que equilibre la innovación tecnológica con la privacidad de las personas, es esencial para evitar un uso indebido de la información. Las herramientas actuales como la Ley 1581 de 2012 proporcionan una base sólida, pero es evidente que deben fortalecerse para abordar los nuevos retos que plantea el tratamiento masivo de datos, en especial cuando se utilizan tecnologías como la IA y el Big Data.
En este contexto, la transparencia en el manejo de datos emerge como un principio fundamental. Los usuarios deben tener acceso claro y sencillo a la información sobre cómo se gestionan sus datos, lo que no solo refuerza la confianza en el sistema, sino que también permite una mayor participación en la toma de decisiones respecto a su privacidad. Del mismo modo, la aplicación efectiva de sanciones por parte de la SIC es esencial para garantizar que se respeten los derechos de los ciudadanos y que las empresas asuman con seriedad sus obligaciones de protección de datos.

A medida que la tecnología avanza, el marco regulatorio deberá evolucionar con ella. Es vital que las normativas continúen adaptándose para mitigar los riesgos asociados con el manejo de grandes volúmenes de información y para proteger de manera efectiva la privacidad de los ciudadanos. Solo a través de una regulación sólida, una supervisión rigurosa y un compromiso firme con la transparencia, será posible enfrentar los desafíos de la era digital, garantizando tanto la protección de los datos personales como el desarrollo tecnológico responsable.