Implicaciones éticas y sociales en la protección de la privacidad de los datos en Colombia

Erika Peñaranda Mejía

Asesor

Jhoana Patricia Romero Leiton

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Ciencia de Datos y Analítica

2025

Dedicatoria

Dedico este trabajo a mi familia, por siempre ser mi refugio, mi fortaleza y mi inspiración constante, gracias porque siempre me demuestran su amor incondicional, y me alientan en cada paso que doy, gracias porque siempre están a mi lado, sin importar si el escenario es de alegría, o de tristeza.

También, dedico este trabajo a mi madre, que vivirá por siempre en mi corazón, tu amor, tus enseñanzas y tu ejemplo de valentía, me acompañaron durante todo este proceso, sé que tu luz sigue y seguirá guiando mi camino.

Y lo dedico a Dios, reconociendo que sin él este título no sería posible.

Resumen

En la actualidad, la protección de la información personal ha adquirido una importancia fundamental debido al auge de la tecnología en las interacciones sociales y empresariales. Este trabajo analiza las implicaciones éticas y sociales de la protección de la privacidad de los datos en el contexto colombiano, destacando las deficiencias en la implementación de las normativas existentes, y los riesgos asociados al mal manejo de la información personal. Para este fin, se realiza un análisis comparativo con marcos normativos internacionales, como el GDPR en la Unión Europea y la LGPD en Brasil, para identificar buenas prácticas aplicables al caso colombiano. Los hallazgos subrayan la importancia de fortalecer el marco normativo, implementar sanciones más severas y fomentar la educación en el manejo ético de los datos personales. Este estudio concluye que Colombia podría fortalecer su marco normativo alineándose con estándares internacionales, como el GDPR, aplicando sanciones económicas proporcionales a los ingresos de las empresas e incentivando certificaciones de buenas prácticas. Esto mejoraría la protección de los datos y la competitividad del país a nivel global.

Palabras clave: Datos personales, Derecho, Ciberseguridad

Abstract

Nowadays, the protection of personal data has become a critical issue due to the rise of technology in social and business interactions. This paper analyzes the ethical and social implications of data privacy protection in the Colombian context, highlighting the shortcomings in the implementation of existing regulations, and the risks associated with the mishandling of personal information. To this end, a comparative analysis is carried out with international regulatory frameworks, such as the GDPR in the European Union and the LGPD in Brazil, to identify good practices applicable to the Colombian case. The findings underline the importance of strengthening the regulatory framework, implementing more severe sanctions, and promoting education in the ethical handling of personal data. This study concludes that Colombia could strengthen its regulatory framework by aligning itself with international standards, such as the GDPR, applying economic sanctions proportional to companies' revenues, and encouraging certifications of good practices. This would improve data protection and the country's competitiveness at a global level.

Keywords: Personal data, Law, Cybersecurity

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Introducción

En esta época donde todo se maneja con datos, es importante identificar esas implicaciones éticas y sociales que puedan generar el no proteger adecuadamente los datos que son recolectados y publicados por diferentes fuentes y organizaciones.

Uno de los ciberataques más comunes que enfrentan tanto individuos como organizaciones es el phishing. A nivel mundial, se generan alrededor de 3.400 millones de correos electrónicos no deseados cada día. Este tipo de ataque utiliza estrategias engañosas para persuadir a las personas a revelar información confidencial o participar en actividades maliciosas mediante correos electrónicos o sitios web fraudulentos. Además, el phishing es responsable del 90% de las violaciones de seguridad de los datos (Kolesnikov. N., 2024).

Cuando existe una violación de los datos tanto la información personal como los interés de los individuos se comprometen porque pueden generar persecución a ciertos perfiles para llegar a ellos o por el contrario pueden ser discriminados, y para las empresas puede ocasionar incluso el cierre de total de las mismas si no son los suficientemente fuertes para levantarse de un hackeo, entonces se debe mantener y manejar una buena ética y seguridad en los datos por el bien de la sociedad en general (Cámara, 2024).

Este panorama obliga a reflexionar sobre la efectividad de las leyes existentes, como la Ley 1581 de 2012, y la necesidad de adoptar mejores prácticas internacionales para garantizar una adecuada protección de los derechos individuales.

Justificación

En este trabajo se analizan las implicaciones éticas y sociales de la protección de la privacidad de los datos en el contexto colombiano, revisando la normativa existente y comparándola con las legislaciones de otros países. Esto es relevante debido al creciente número de riesgos asociados con la gestión y el uso indebido de la información personal en la era digital.

En Colombia, la gestión de la información personal está regulado por la Ley 1581 de 2012. Esta legislación se aplica tanto a los procesos de tratamiento de datos llevados a cabo dentro del territorio nacional como a aquellos en los que el responsable o encargado del tratamiento, aun estando fuera del país, deba acatar la normativa colombiana debido a tratados internacionales y disposiciones legales vigentes (Función Pública, 2012).

Esta normativa exige que las entidades u organizaciones que recopilan datos personales garanticen que dicha información no sea publicada ni difundida a través de internet o medios de comunicación masiva. Asimismo, es fundamental que adopten las medidas técnicas, humanas y administrativas adecuadas para garantizar la seguridad de los registros, previniendo su modificación, extravío, acceso, consulta, uso o manipulación sin autorización o de manera fraudulenta (Función Pública, 2012).

A pesar de estas disposiciones legales, los datos personales en Colombia siguen siendo vulnerables, donde los datos pueden ser expuestos afectando la ética y socialmente a la población. En Colombia para el año 2023 sufrieron 12.000 millones de intentos de ciberataques, estos pueden desencadenar pagos de grandes cantidades de millones de pesos en sobornos, y poner otras manos información confidencial de los usuarios, sin tener nuestra previa autorización para el tratamiento de dichos datos (CCIT, 2024).

Además, esta situación afecta de manera considerable la confianza de los ciudadanos en las instituciones y la sensación de seguridad en el ámbito digital. Por ello, es fundamental evaluar las fallas en la aplicación de las normativas vigentes y desarrollar estrategias efectivas que fortalezcan la protección de los datos personales.

Objetivos

Objetivo General

Analizar las leyes, dilemas éticos y efectos sociales relacionados con la protección de los datos personales en Colombia, comparándolos con las normativas y prácticas de otros países. Esto se realizará con el fin de proponer recomendaciones políticas que permitan el fortalecimiento de las normativas nacionales y garanticen una mejor protección de los derechos individuales.

Objetivos Específicos

Investigar las leyes y regulaciones existentes sobre la protección de los datos en Colombia.

Realizar una revisión bibliográfica de las leyes de protección de datos existentes en otros países diferentes a Colombia, tanto países desarrollados como en desarrollo.

Investigar los dilemas éticos en la recolección, almacenamiento y uso de los datos personales en Colombia.

Analizar cómo el uso de los datos puede afectar a diferentes grupos sociales.

Generar recomendaciones dirigidas a nivel político, para fortalecer el marco normativo de la protección de los datos en Colombia. Estas recomendaciones estarán basadas en el análisis comparativo de las leyes internacionales, para detectar mejores prácticas internacionales en la protección de los datos.

Protección de Datos Personales en Colombia: Análisis Comparativo, Dilemas Éticos y Recomendaciones Normativas

Empezaremos por abordar algunos conceptos para entender porque existen Implicaciones éticas y sociales en la protección de la privacidad de los datos.

La privacidad de los datos se basa en el derecho de cada individuo a controlar su información personal, lo que incluye la facultad de decidir cómo las organizaciones la recopilan, almacenan y utilizan. Este control es fundamental para garantizar la seguridad de los datos, donde se garantiza que solo las personas adecuadas puedan acceder a los datos, y no se presente algún acceso no autorizado o uso indebido (IBM, 2023).

La ética en la gestión de datos se refiere a un conjunto de principios que guían el uso responsable y apropiado de la información dentro de una organización. Estas directrices permiten a los responsables, partes interesadas y empleados comprender las implicaciones éticas asociadas al tratamiento de los datos (PureStorage, 2024). La ética de los datos se basa en tres principios: El de Transparencia, el de Responsabilidad y el de Equidad (PureStorage, 2024).

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como redes informáticas o bases de datos, con el propósito de perjudicar a personas, organizaciones o empresas. Estas acciones pueden comprometer tanto los dispositivos y sistemas conectados a la red, interrumpiendo su funcionamiento, como las bases de datos que contienen información sensible, la cual puede ser interceptada, robada o utilizada con fines de extorsión. (Iberdrola, 2024).

Un recorrido Sobre las Leyes y Regulaciones de la Protección de los Datos en Colombia

Dentro del marco legal colombiano, la Ley 1581 de 2012 tiene como propósito garantizar el derecho constitucional de todas las personas a acceder, modificar y rectificar los datos almacenados sobre ellas en registros o bases de información (Función Pública, 2012).

El artículo 4, inciso f, sobre el principio de acceso y circulación restringida en el tratamiento de datos personales, establece que solo las personas autorizadas pueden gestionar esta información. Además, salvo que se trate de datos de carácter público, no podrá estar disponible en internet ni en medios de comunicación masiva (Función Pública, 2012).

Además, el inciso g, referente al principio de seguridad, dispone que quien gestione el tratamiento de los datos debe aplicar las medidas técnicas, humanas y administrativas necesarias para garantizar su protección, evitando su alteración, pérdida o acceso no autorizado (Función Pública, 2012).

Algunas categorías de datos personales se consideran especiales, como los datos sensibles, los cuales están relacionados con la intimidad del titular. El uso indebido de esta información puede generar discriminación. Entre ellos se encuentran aquellos que revelan el origen racial o étnico, las orientaciones políticas o religiosas, así como datos sobre salud, vida sexual y características biométricas (Función Pública, 2012).

Las personas poseen el derecho de retirar su consentimiento y solicitar la eliminación de sus datos cuando su tratamiento no respete los principios, derechos y garantías estipulados en la Constitución y la legislación vigente (Función Pública, 2012).

También es relevante destacar la Ley 1266 de 2008 en Colombia, conocida como la Ley de Habeas Data, la cual establece normas para el manejo de datos personales en registros digitales, con especial énfasis en los sectores financiero, crediticio, comercial y de servicios. Su

propósito fundamental es asegurar la protección de los datos personales y regular su recolección, almacenamiento, uso y difusión (Función Pública, 2008).

La Ley 1273 de 2009 en Colombia, conocida como la Ley de Delitos Informáticos, tiene como finalidad resguardar la información y los datos personales en el ámbito digital, además de penalizar los delitos vinculados al uso indebido de sistemas informáticos y redes de datos. Y menciona sanciones que varían según el delito, estas sanciones pueden ser multas y prisión de hasta 10 años dependiendo de la gravedad del delito (Función Pública, 2009).

Asimismo, Colombia ha adoptado diversas prácticas internacionales para fortalecer el Sistema de Gestión de la Seguridad de la Información (SGSI). Entre las más relevantes se encuentra la norma ISO/IEC 27001, que permite:

- Implementación de mecanismos de control para la gestión de datos personales e información sensible, mediante medidas de seguridad y controles adecuados.
- Optimización y eficacia en la administración y tratamiento de los datos personales.
- Garantía de transparencia y cumplimiento normativo durante las investigaciones realizadas por los organismos de control en materia de protección de datos (Fonte Estudio Jurídico, 2018).

Perspectiva Internacional Sobre la Protección de Datos: Una Revisión Comparativa de Normativas en Países Desarrollados y en Desarrollo

La privacidad de los datos personales se empezó a convertir en un derecho fundamental en la década de 1940 con el crecimiento del internet y el desarrollo de la tecnología. La privacidad de los datos hace referencia al procedimiento mediante el cual se hace una recopilación, administración, distribución y almacenamiento de la información personal de una

persona. En algunos países, existen leyes y regulaciones sólidas que brindan a las personas salvaguardas para sus datos personales (Privacy HQ, 2024).

Los 5 países con mejores políticas de privacidad de datos son La Unión Europea, Islandia, Noruega, Japón, Suiza (Privacy HQ, 2024).

La Unión Europea encabeza la lista debido a la implementación del Reglamento General de Protección de Datos (GDPR por sus siglas en inglés). Esta normativa, considerada la más estricta en materia de privacidad y seguridad a nivel mundial, fue adoptada por la UE y establece obligaciones para organizaciones de cualquier parte del mundo que recopilen o procesen datos de ciudadanos europeos. Esta norma entro en vigor desde el 25 de mayo de 2018, el GDPR impone sanciones significativas a quienes no cumplan con sus estándares, con multas que pueden alcanzar decenas de millones de euros. Con esta regulación, Europa reafirma su compromiso con la protección de la privacidad y la seguridad de los datos (GDPR.EU, 2024).

En Japón, se están llevando a cabo esfuerzos por mejorar su ciberseguridad transformando sus capacidades de defensa en tierra, mar, aire y espacio exterior, lo que marca un cambio en su estrategia de seguridad nacional y regional. Japón está liderando activamente los esfuerzos para crear una red contra los ciberataques en la región del Indo-Pacífico, con el objetivo de mejorar sus alianzas y protegerse contra las amenazas cibernéticas (Observer Research Fundation, 2024).

La Superintendencia de Industria y Comercio (SIC) estableció una serie de criterios para identificar qué países cuentan con un nivel adecuado de protección de datos. Estos estándares incluyen:

- La existencia de normativas que regulen el tratamiento de datos personales.
- La incorporación de principios legales aplicables a la materia.

- El reconocimiento normativo de los derechos de los titulares de los datos.
- La definición de las obligaciones de los administradores y gestores del tratamiento de datos.
- La disponibilidad de mecanismos judiciales y administrativos que garanticen la protección efectiva de los derechos de los titulares y el cumplimiento de la legislación.
- La presencia de entidades encargadas de supervisar y regular el cumplimiento de las normas de protección de datos (Ámbito Jurídico, 2017).

Basándose en estos estándares mínimos, los países que poseen un nivel adecuado de políticas de protección de datos incluyen Alemania, Costa Rica, Estados Unidos, Francia e Italia (Ámbito Jurídico, 2017).

En América Latina, Brasil se destaca como uno de los países pioneros en la implementación de nuevas leyes de protección de datos. En 2020, entró en vigor una normativa que incorpora elementos del Reglamento General de Protección de Datos (GDPR) de la Unión Europea, estableciendo estrictas obligaciones de cumplimiento para las empresas que gestionan datos o prestan servicios a personas en Brasil (TMF Group, 2019).

La protección de sus datos personales es fundamental, estos representan su identidad dentro de la sociedad y forman parte de su personalidad. Por ello, deben ser gestionados de manera justa y segura, respetando las expectativas legítimas. En Brasil, la Ley General de Protección de Datos Personales (LGPD) tiene como objetivo asegurar que el tratamiento de los datos se realice de manera legal, apropiada y con los niveles de seguridad adecuados (ANPD, 2024).

Dilemas Éticos en el Manejo de Datos Personales en Colombia: Retos en la Recolección, Almacenamiento y Uso

Uno de los principales desafíos que enfrenta Colombia en la recolección de datos personales, es asegurar que las empresas y organizaciones que los recopilan cumplan con las normativas establecidas para su tratamiento, como la Ley 1581 de 2012 de Habeas Data. Esta normativa tiene como propósito asegurar el derecho constitucional de cada individuo a consultar, modificar y rectificar la información que se encuentra registrada sobre ellos en bases de datos o archivos. Además, es fundamental que se cuente con el consentimiento informado de los usuarios y se fomente la confianza en el manejo adecuado de los datos recopilados (Función Pública, 2012).

En el almacenamiento de los datos personales se pueden presentar diferentes retos, primero que todo inversiones en ciberseguridad, ya que cualquier organismo que capte datos puede ser víctima de ataques cibernéticos, robo y exposición de la información, por lo cual es importante implementar medidas de seguridad. Además, otros retos están en que las empresas u organizaciones tengan el personal lo suficientemente capacitado en el manejo de datos y asumir costos de infraestructura, lo que puede resultar costoso para ciertas empresas (Sealpath, 2024).

El uso de los datos recolectados de forma transparente es muy importante para tomar decisiones tanto en los ámbitos micro y macro. Por ejemplo, en un país, el uso de los datos recolectados puede ayudar a crear políticas públicas y a optimizar servicios como el transporte y la salud, entre otros; en el ámbito micro puede ayudar a crecimiento empresarial y al aumento de inversiones, entre otros. Pero para ello es importante generar conciencia desde la recolección de los datos, además de que los datos sean recolectados cumpliendo las respectivas leyes, estos

deben tener homogeneidad, y actualizaciones pertinentes, para generar análisis y resultados más acertados (Banco Interamericano de Desarrollo, 2017).

Nos encontramos en una sociedad impulsada por los datos, donde muchas de nuestras actividades diarias dependen de su recopilación, uso e intercambio con empresas o entidades gubernamentales. Asimismo, en internet compartimos información constantemente, ya sea al realizar compras en línea o al interactuar en redes sociales (ANPD, 2024).

La ética en el manejo de los datos es fundamental, ya que permite a las organizaciones mitigar los riesgos asociados a la privacidad y optimizar la experiencia de los usuarios sin afectar la confidencialidad de su información personal. Al seguir estos principios, las organizaciones pueden:

- Establecer un marco regulador universal que delimite el uso permitido y restringido de los datos.
- Proteger la confidencialidad de los datos de los consumidores, cumpliendo con normativas estipuladas.
- Fomentar la confianza de los clientes mediante la adopción de un código de conducta basado en principios éticos, asegurando un uso responsable y transparente de sus datos (PureStorage, 2024).

Implicaciones Sociales del Uso de Datos: Una Mirada a los Efectos en Diversos Grupos Poblacionales

La protección de datos es esencial no solo para los ciudadanos, sino también para la economía y la sociedad en su conjunto. Brinda a las personas el control sobre su información, fortaleciendo su derecho a la libertad de expresión, el acceso a la información y la protección de la intimidad, el honor y la imagen (ANPD, 2024).

En esta sección se presentan antecedentes que ejemplifican casos de ciberataques que han experimentado empresas muy importantes en Colombia, y cuáles fueron las implicaciones éticas y sociales de esos ataques.

Ciberataque a Grupo Keralty en el 2022, este ciberataque afectó a millones de usuarios, ya que por este hecho se presentó afectaciones e inconvenientes en todas sus plataformas. Para contextualizar Grupo Keralty presta servicios de salud bajo la EPS Sanitas, el hecho de que haya sido víctima de ciberataque puso en riesgo la información personal de carácter confidencial de los usuarios ya que el objetivo del ataque fue secuestro de la información (Portafolio, 2022).

Ciberataque a la Pontificia Universidad Javeriana en el 2021, este hecho se presentó en las sedes de Bogotá y Cali, lo cual tuvo que suspender sus sistemas informativos e irlos habilitando de forma gradual mientras se determinaba que ya fuera un ambiente seguro. Los Hackers había secuestrado 200 teras de información y estaban pidiendo a cambio 25 mil dólares para devolverlos (El Colombiano, 2021).

Ciberataque a EPM Empresas Públicas de Medellín en el 2022, este es otro ejemplo más Hackeo, ya que con esto se pueden ocasionar más ciberdelitos, como la suplantación de la página web, captando tanto información de los métodos de pago de todo aquel que le pague a la empresa y fuga del dinero ya que nunca llegara al verdadero destinatario, además perjudicando los servicios prestados como reconexiones, recargas de energía y agua, procesos de pagos, facturación y contratación (El Tiempo, 2022).

Ciberataque a Salud Total en 2024: El 29 de enero de 2024, se informó que la EPS sufrió un ataque cibernético que comprometió sus plataformas digitales, afectando el acceso a información esencial para su operación diaria. Ante esta situación, la entidad tuvo que

implementar medidas para reducir el impacto en sus más de 4.8 millones de usuarios (Infobae, 2024).

Este tipo de ataques puede tener consecuencias significativas, ya que no solo impactan a las personas, sino que también pueden poner en riesgo la continuidad de las empresas. Una pequeña empresa podría verse obligada a cerrar sus operaciones en los seis meses posteriores a un ataque cibernético. Las grandes empresas, aunque puedan resistir el impacto, lo hacen enfrentándose a un costo considerable. Incluso las multinacionales pueden sufrir pérdidas financieras, deterioro de su reputación crediticia y una reducción en su productividad (Easy Dmar, 2024).

Otras consecuencias a las que se está expuesto cuando existe una violación de los datos son robo de identidad, pérdidas financieras como lo hemos mencionado, es muy común que cuando secuestran los datos pidan un rescate ocasionando pérdidas financieras para la organización afectada, sin embargo, también los individuos en ciberataques o hackeos pierden dinero, para las empresas además también afecta en la productividad, pérdida de clientes, fallo en la privacidad, daño en la reputación y pérdida de propiedad intelectual (Easy Dmar, 2024).

Algunas de las amenazas a las que se enfrenta la privacidad de los datos es, amenazas del gobierno donde muchos países buscan equilibrar la privacidad individual con la necesidad de seguridad nacional, están las amenazas comerciales donde las organizaciones comerciales buscan tener ventajas competitivas y amenazas criminales donde los datos personales robados se ponen en venta en internet (Privacy HQ, 2024).

En este contexto donde todos somos vulnerables ante una violación de los datos personales, es importante mencionar que la privacidad es un derecho, y a través de ese derecho se refuerzan otros derechos, “*el derecho a la privacidad se presenta como un pasaporte que*

refuerza otros derechos, en la red y fuera de la red, incluyendo los derechos a la igualdad y a la no discriminación, y a la libertad de expresión y reunión." (Naciones Unidas, 2018, párr. 3).

No obstante, muchas personas no siempre son conscientes de la información que están proporcionando ni de quién la está recibiendo. A menudo, desconocen que, en el entorno digital, cuando un servicio es gratuito, en realidad no somos el cliente, sino el producto (Naciones Unidas, 2018). Un ejemplo de esto es la venta de datos de usuarios de Facebook, donde se recolectó información de 1.500 millones de usuarios mediante una técnica conocida como scraping. El web scraping es un método que permite extraer grandes volúmenes de información de sitios web utilizando scripts automatizados (Welivesecurity, 2021).

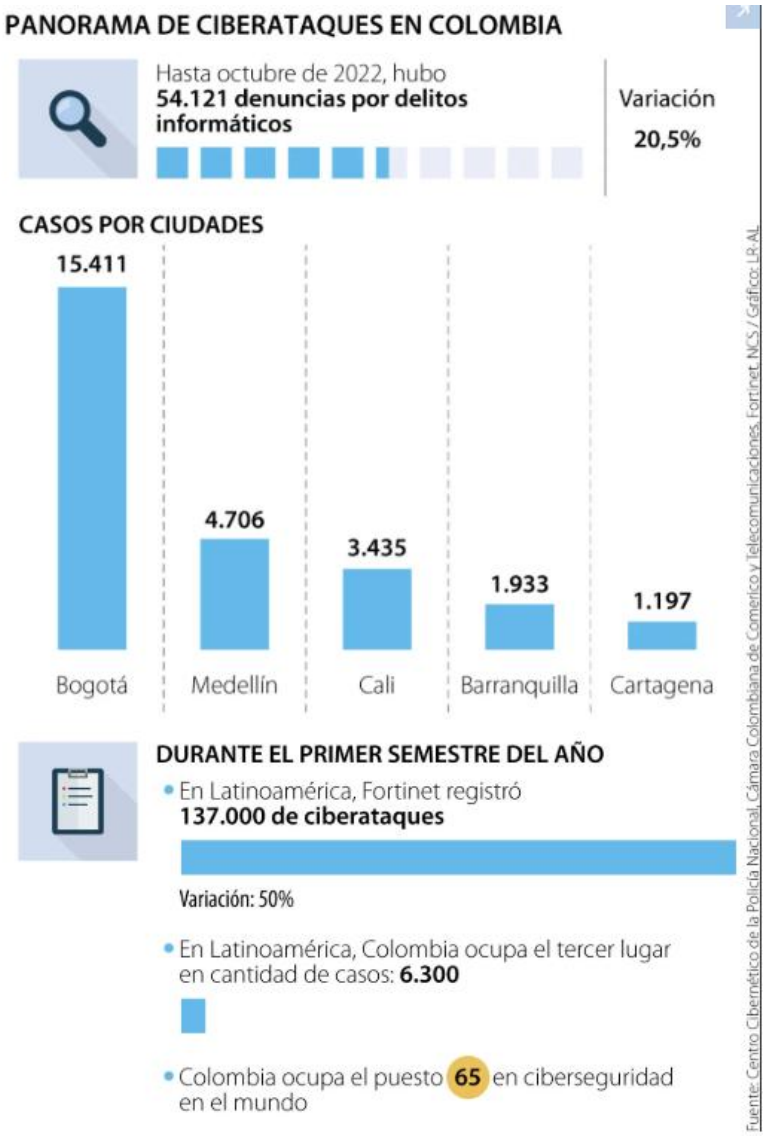
En Colombia, se registran aproximadamente 79 casos diarios de vulneración a la protección de datos personales. Esta problemática se evidencia en situaciones como recibir llamadas de empresas con las que no se tiene relación alguna o intentos de estafa telefónica, entre otros. Estas prácticas representan las principales razones por las cuales los ciudadanos presentan denuncias (Uniandes, 2023). De esta manera, se afecta nuestro derecho a la protección y privacidad de los datos. Para que un derecho sea efectivo en la práctica, no basta con su regulación; es fundamental que las entidades responsables cumplan con sus obligaciones legales (Uniandes, 2023).

En el informe de gestión sobre la protección de datos del año 2021, la Superintendencia de Industria y Comercio (SIC) informó que recibió un total de 28.610 quejas ciudadanas, con un promedio mensual de 2.384. De acuerdo con el reporte, el 90% de estas denuncias estuvieron relacionadas con posibles incumplimientos de la Ley Estatutaria 1266 de 2008 (Habeas Data financiero), mientras que el 10% restante correspondió a infracciones a la Ley Estatutaria 1581

de 2012 (Ley General de Protección de Datos). La queja más recurrente fue la ausencia de autorización para la recolección y uso de datos (SIC, 2021).

Figura 1

Panorama de Ciberataques en Colombia



Nota. Estadísticas de ciberataques en Colombia para el año 2022, la información proviene de La República (2022).

En el 2022 La República publicó un artículo sobre los ataques cibernéticos en Colombia, donde se puede evidenciar que en Colombia la ciudad que más casos registra de ciberataques es Bogotá, seguida de Medellín y Cali, además Colombia ocupa el tercer lugar en cantidad de casos en Latinoamérica.

Según La República, el comercio electrónico es una de las industrias más vulnerables, enfrentando riesgos que pueden generar pérdidas significativas o incluso millonarias. Por ello, se destaca la importancia de que el Gobierno Nacional y las autoridades competentes implementen medidas más efectivas de seguridad cibernética. Estas acciones deben enfocarse en proteger tanto a la industria como, especialmente, los datos personales de los ciudadanos que realizan compras en línea, frente a este tipo de ataques (La República, 2022).

Recomendaciones Políticas para el Fortalecimiento de la Normativa Colombiana de Protección de Datos

La protección de datos personales se ha convertido en una prioridad a nivel mundial, impulsada por la creciente necesidad de preservar la privacidad y seguridad en un entorno digital cada vez más complejo. Para enfrentar este desafío, varios países han implementado marcos regulatorios específicos, como el GDPR en la Unión Europea, así como la adopción de estándares internacionales en naciones como Brasil y Japón. En este contexto, es fundamental realizar un análisis comparativo de las normativas vigentes con el fin de identificar áreas de mejora en la legislación colombiana, permitiendo así fortalecer la protección de los datos personales y alinearse con las mejores prácticas internacionales.

Tabla 1

Cuadro Comparativo Internacional de Normas de Protección de Datos con Colombia

Aspecto / País	Colombia (Ley 1581 de 2012 y Ley 1273 de 2009)	Latinoamérica (Brasil - LGPD)	Unión Europea (GDPR)	Japón	Otros Países con Buenas Políticas (Alemania, EE. UU., Costa Rica, etc.)
Marco Jurídico/ Cooperación	Ley 1581 de 2012 (Normativa sobre la protección de datos personales) y Ley 1273 de 2009 (Legislación sobre delitos informáticos).	.LGPD (Ley General de Protección de Datos), implementada desde el año 2020.	GDPR (General Data Protection Regulation), en vigor desde mayo de 2018.	Ley de Protección de Información Personal (APPI, 2003) y cooperación internacional a través del programa Japón-OTAN (2020).	Normativas específicas según cada país, estableciendo reglas para el manejo de datos personales.
Alcance	Aplica a personas naturales o jurídicas que traten datos personales dentro del territorio colombiano, incluso bajo contrato.	Obliga a empresas que procesan datos o brindan servicios a personas en Brasil.	Aplicación extraterritorial; afecta a organizaciones que recopilan datos de ciudadanos de la UE, sin importar su ubicación.	Se aplica a todas las organizaciones que recolectan, gestionan o tratan datos personales de residentes en Japón.	Depende del país; algunos, como EE. UU., tienen leyes sectoriales.

Aspecto / País	Colombia (Ley 1581 de 2012 y Ley 1273 de 2009)	Latinoamérica (Brasil - LGPD)	Unión Europea (GDPR)	Japón	Otros Países con Buenas Políticas (Alemania, EE. UU., Costa Rica, etc.)
Principios Clave	Legalidad, finalidad, libertad, transparencia, seguridad, confidencialidad y acceso restringido.	Transparencia, consentimiento informado, adecuación, necesidad y seguridad.	Transparencia, limitación del propósito, minimización de datos, seguridad y responsabilidad.	Consentimiento informado, limitación de uso, seguridad y responsabilidad.	En general, se exigen principios como seguridad, consentimiento y limitación de uso.
Derechos de los Titulares	Acceso, rectificación, supresión, revocatoria del consentimiento y consulta sobre el uso de los datos.	Derechos similares a los del GDPR, incluyendo acceso, corrección y eliminación de datos.	Acceso, rectificación, borrado (derecho al olvido), portabilidad de datos, oposición, entre otros.	Acceso, rectificación, eliminación, y limitación del uso de datos personales.	Varían según el país; algunos reconocen derechos como acceso y rectificación.
Sanciones por Incumplimiento	Sanciones de hasta 2.000 salarios mínimos legales mensuales vigentes (SMMLV) o la interrupción de actividades vinculadas al manejo de datos.	Multas administrativas de hasta el 2% de los ingresos globales anuales.	Sanciones de hasta 20 millones de euros o el equivalente al 4% de la facturación anual global.	Multas administrativas que pueden alcanzar hasta 100 millones de yenes, dependiendo de la gravedad del incumplimiento.	Multas específicas según el país, menos severas en comparación con el GDPR.

Aspecto / País	Colombia (Ley 1581 de 2012 y Ley 1273 de 2009)	Latinoamérica (Brasil - LGPD)	Unión Europea (GDPR)	Japón	Otros Países con Buenas Políticas (Alemania, EE. UU., Costa Rica, etc.)
Supervisión y Cumplimiento	Supervisado por la Superintendencia de Industria y Comercio (SIC).	Supervisado por la ANPD (Autoridad Nacional de Protección de Datos) en Brasil.	Supervisado por autoridades nacionales independientes en cada estado miembro de la UE.	Supervisado por la Comisión de Protección de Información Personal (PPC, establecida en 2016).	Supervisión varía según el país; algunas naciones cuentan con entidades específicas.
Relevancia Internacional	Marco sólido para América Latina, pero enfrenta desafíos en implementación y sensibilización del público sobre sus derechos.	Inspirado en el GDPR; destaca como la regulación más completa en América Latina.	Es el estándar más influyente en políticas de protección de datos a nivel mundial.	Se alinea con estándares internacionales y coopera en ciberseguridad y protección de datos en el marco de la OTAN.	Algunos países alcanzan niveles adecuados según estándares internacionales.

Nota. La información recopilada proviene de Función Pública (2012), Función Pública (2009), TMF Group (2019) e Intersoft Consulting (2024).

A partir del cuadro comparativo, se pueden identificar políticas que podrían ser una oportunidad de mejora en la normativa colombiana de la protección de datos personales.

Por ejemplo, incluir el alcance extraterritorial como lo tiene la Unión Europea donde se podría obligar a las empresas extranjeras a cumplir con las normativas colombianas si se maneja datos de ciudadanos colombianos.

Incluir multas que puedan ser proporcionales a los ingresos de las empresas que cometen la infracción.

Promover que las empresas se certifiquen en el cumplimiento de buenas prácticas en la protección de datos.

Asimismo, es fundamental desarrollar campañas de concientización dirigidas a ciudadanos y a entidades tanto públicas como privadas, con el objetivo de informarles sobre sus derechos y responsabilidades en cuanto a la protección de datos personales.

Conclusiones

Este estudio llevó a cabo una revisión de la literatura sobre la gestión de la protección de datos en Colombia, analizando también los impactos sociales derivados de la falta de ética en la recopilación, almacenamiento y uso de la información personal. Además, se comparó cómo son las normas adoptadas en otros países para el manejo de la protección de los datos. Para este fin se consultaron diversas fuentes web de Colombia y el exterior.

Se realizó un análisis de las normativas vigentes en Colombia sobre la protección de datos, identificando como más relevantes la Ley 1581 de 2012, la cual garantiza el derecho constitucional de las personas a acceder, actualizar y corregir la información almacenada sobre ellas en bases de información o archivos (Función Pública, 2012), La Ley 1273 de 2009 en Colombia, denominada Ley de Delitos Informáticos, tiene como propósito salvaguardar la información y los datos personales en el ámbito digital, además de penalizar los delitos asociados al uso inadecuado de sistemas informáticos y redes de datos (Función Pública, 2009).

En la revisión de las leyes de protección de datos existentes en otros países se encontró, que aquellos que pertenecen a la Unión Europea son los que poseen las políticas de privacidad y seguridad de datos más estricta del mundo, y que Brasil siendo un país latinoamericano, adoptó desde el 2020 algunas prácticas incluidas en el de GDPR (General Data Protection Regulation) de la Unión Europea; además también se resalta en el ámbito internacional a Japón y como ellos han creado una cooperación entre países para la ciberseguridad y protección de datos.

Se examinaron los conflictos éticos asociados a la recolección, gestión y utilización de la información personal en Colombia, reconociendo que vivimos en una sociedad impulsada por la información, donde gran parte de las actividades diarias implican la recolección, procesamiento y intercambio de datos con empresas y entidades gubernamentales (ANPD, 2024). La ética en el

manejo de datos es fundamental, ya que permite a las organizaciones gestionar los riesgos vinculados a la privacidad y optimizar la experiencia de los usuarios sin poner en peligro la confidencialidad de su información personal (PureStorage, 2024).

Se analizó cómo el uso de los datos puede afectar a diferentes grupos sociales, debido a que los ataques cibernéticos generan grandes consecuencias no solo a las personas, sino que pueden tener la capacidad de destruir empresas (Easy Dmar, 2024). La protección de datos es fundamental tanto para las personas como para la economía y la sociedad en su conjunto. Permite a los ciudadanos tener control sobre su información y refuerza derechos esenciales como la libertad de expresión, el acceso a la información, la privacidad, el honor y la protección de la imagen (ANPD, 2024). Dado que todos estamos expuestos a riesgos, es fundamental implementar políticas más rigurosas y contar con entidades de control que aseguren el cumplimiento de los derechos y responsabilidades en materia de protección de datos en Colombia.

Colombia puede mejorar su normativa adoptando prácticas internacionales más estrictas, como adoptar las sanciones económicas tomando como modelo la Unión Europea y Brasil, donde las sanciones son basadas en porcentajes de los ingresos globales de las empresas, lo cual hace que la multa sea más significativa y efectiva para promover el cumplimiento de la normativa en materia de la protección de datos. También Colombia podría adoptar la promoción de certificados de buenas prácticas para incentivar el cumplimiento por parte de las empresas.

Colombia tiene la oportunidad de modernizar su normativa de protección de datos al alinearse con estándares internacionales como el GDPR. Esto no solo protegería mejor a los ciudadanos, sino que también fortalecería la confianza y la competitividad del país en el ámbito global.

A pesar de que este trabajó presentó un análisis preliminar sobre la protección de datos personales en Colombia, destacando las implicaciones éticas y sociales de su manejo, enfrenta varias limitaciones. En primer lugar, la literatura disponible sobre normatividad en el contexto colombiano es limitada, lo que restringe el alcance del análisis. Las leyes analizadas, como la Ley 1581 de 2012 y la Ley 1273 de 2009, son relevantes, pero representan un marco que ha permanecido constante y no aborda de manera suficiente los desafíos actuales en ciberseguridad. Además, no se identificó una solución específica o clara para superar las deficiencias existentes en la implementación normativa, lo que sugiere la necesidad de estudios más detallados. Otra limitación significativa fue el tiempo disponible para este proyecto, lo que limitó la profundidad del análisis comparativo con normativas internacionales.

En el futuro, se recomienda ampliar esta investigación con documentación aun en otros idiomas, para abarcar una perspectiva global más inclusiva y explorar los impactos de las normativas en muchos más países. También, sería valioso investigar las percepciones ciudadanas sobre la privacidad de los datos y su confianza en las instituciones. Finalmente, al comparar la normativa colombiana con la de otros países, se pueden identificar buenas prácticas y marcos de regulación más avanzados que podrían servir de referencia para mejorar el sistema colombiano. Esto no solo permitirá mitigar los riesgos asociados con los ciberataques, sino también garantizar un entorno más ético y seguro para la gestión de la información personal.

Referencias

Ámbito Jurídico. (2017). *Estos son los países con un nivel adecuado de protección de datos personales*. Https://Www.Ambitojuridico.Com/Noticias/General/Mercantil-Propiedad-Intelectual-y-Arbitraje/Estos-Son- Los-Paises-Con-Un-Nivel

ANPD. (2024). *Cómo proteger sus datos personales*. Chrome-Extension://Efaidnbmnnnibpcajpcglclefindmkaj/Https://Www.Gov.Br/Anpd/Pt-Br/Documentos-e-Publicacoes/Guia_senacon_espanhol.Pdf

Banco Interamericano de Desarrollo. (2017). *El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el Caribe*. Https://Publications.Iadb.Org/Es/Node/17863

Cámara. (2024). *Los ciberataques son la principal causa de cierre del 57% de las pymes*. Https://Camaranavarra.Com/2024/10/18/Los-Ciberataques-Son-La-Principal-Causa-de-Cierre-Del-57-de-Las-Pymes/#:~:Text=octubre-,Los%20ciberataques%20son%20la%20principal%20causa,Del%2057%25%20de%20las%20pymes

CCIT. (2024). *Camara Colombiana de Informatica y Telecomunicaciones. Colombia sufrió 12.000 millones de intentos de ciberataques en 2023 según reporte de Fortinet*. Https://Www.Ccit.Org.Co/Blog/Colombia-Sufrio-12-000-Millones-de-Intentos-de-Ciberataques-En-2023-Segun-Reporte-de-Fortinet

Easy Dmar. (2024). *¿Cuáles son las consecuencias de una violación de datos?* Https://Easydmarc.Com/Blog/Es/Cuales-Son-Las-Consecuencias-de-Una-Violacion-de-Datos/#:~:Text=Una%20de%20las%20consecuencias%20%C3%A9ticas,Investigaciones%20formales%20y%20denuncias%20p%C3%BAblicas

El Colombiano. (2021). *Atacan a la Javeriana: cibersecuestro de sus datos en dos ciudades.* Https://Www.Elcolombiano.Com/Colombia/Secuestran-Datos-de-La-Universidad-Javeriana-En-Colombia-LB16067491

El Tiempo. (2022). *Expertos hablan sobre la gravedad y riesgos del ciberataque que sufrió EPM*. Https://Www.Eltiempo.Com/Colombia/Medellin/Medellin-La-Gravedad-y-Riesgos-Del-Ciberataque-Que-Sufrio-Epm-729517

Fonte Estudio Jurídico. (2018). *El reto corporativo en el tratamiento de los datos personales.* Https://Fonte.Com.Co/El-Reto-Corporativo-En-El-Tratamiento-de-Los-Datos-Personales-Recomendaciones/

Función Pública. (2008). *Ley 1266 de 2008*. Https://Www.Funcionpublica.Gov.Co/Eva/Gestornormativo/Norma.Php?I=34488#0

Función Pública. (2009). *Ley 1273 de 2009*. Https://Www.Funcionpublica.Gov.Co/Eva/Gestornormativo/Norma.Php?I=34492

Función Pública. (2012). *Ley estatutaria 1581 de 2012*. Https://Www.Funcionpublica.Gov.Co/Eva/Gestornormativo/Norma.Php?I=49981

GDPR.EU. (2024). *What is GDPR, the EU's new data protection law?* Https://Gdpr.Eu/What-Is-Gdpr/

Iberdrola. (2024). *Ataques cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos?* Https://Www.Iberdrola.Com/Innovacion/Ciberataques

IBM. (2023). *¿Qué es la privacidad de los datos?* . Https://Www.Ibm.Com/Mx-Es/Topics/Data-Privacy

Infobae. (2024). *Salud Total EPS denunció ser víctima de ataque cibernético: confirmó a sus usuarios si sus servicios se vieron afectados*.

Https://Www.Infobae.Com/Colombia/2024/01/30/Salud-Total-Denuncio-Ser-Victima-de-Ataque-Cibernetico-Eps-Confirmo-a-Sus-Usuarios-Si-Sus-Servicios-Se-Vieron-Afectados/

Intersoft Consulting. (2024). *General Data Protection RegulationGDPR*. Https://Gdpr-Info.Eu/

Kolesnikov. N. (2024). *Techopedia. 50 Estadísticas Clave de Ciberseguridad para Julio de 2024*. Https://Www.Techopedia.Com/Es/Estadisticas-Ciberseguridad

La República. (2022). *Los ciberataques suman 54.121 casos en lo que va del año y han crecido más de 20%*. Https://Www.Larepublica.Co/Empresas/Los-Ciberataques-Suman-54-121-Casos-En-Lo-Que-va-Del-Ano-y-Han-Crecido-Mas-de-20-3509163

Naciones Unidas. (2018). *Artículo 12: derecho a la intimidad*. Https://News.Un.Org/Es/Story/2018/11/1446671

Observer Research Fundation. (2024). *From reactive to proactive: Japan's advances in cybersecurity and cyber defence strategies*. Https://Www.Orfonline.Org/Expert-Speak/from-Reactive-to-Proactive-Japan-s-Advances-in-Cybersecurity-and-Cyber-Defence-Strategies#:~:Text=The%20foundation%20for%20Japan's%20cybersecurity,Headquarters%20and%20a%20Cybersecurity%20Council

Portafolio. (2022). *Ataque informático a Sanitas no comprometió información de usuarios.* . Https://Www.Portafolio.Co/Negocios/Empresas/Eps-Sanitas-Detalles-Del-Ciberataque-Que-Sufrio-Grupo-Keralty-575968

Privacy HQ. (2024). *Clasificación de privacidad de datos: los 5 primeros y los 5 últimos países*. Https://Privacyhq.Com/News/World-Data-Privacy-Rankings-Countries/

PureStorage. (2024). *¿Qué es la ética de los datos y de qué modo el almacenamiento puede mejorar las mejores prácticas éticas?* Https://Www.Purestorage.Com/Es/Knowledge/What-Is-Data-Ethics.Html#:~:Text=La%20%C3%A9tica%20de%20los%20datos%20aborda%20las%20conductas%20relacionadas%20con,Tecnolog%C3%ADas%2C%20para%20evitar%20los%20sesgos

Sealpath. (2024). *10 Preocupaciones en seguridad de datos de las organizaciones y CISOs*. Https://Www.Sealpath.Com/Es/Blog/Desafios-Seguridad-Datos-Empresas/

SIC. (2021). *Más de 28 mil quejas recibió la Superindustria en 2021 por protección de datos personales*. Https://Www.Sic.Gov.Co/Slider/M%C3%A1s-de-28-Mil-Quejas-Recibi%C3%B3-La-Superindustria-En-2021-Por-Protecci%C3%B3n-de-Datos-Personales

TMF Group. (2019). *Las leyes sobre protección de datos en América Latina*. Https://Www.Tmf-Group.Com/Es-Co/Noticias-Perspectivas/Articulos/Formacion-Administracion-Empresas/Leyes-Proteccion-Datos-America-Latina/

Uniandes. (2023). *Cada día, en Colombia se presentan cerca de 79 casos de violación de protección de datos personales*. Https://Wwwadmin.Uniandes.Edu.Co/Es/Cada-D%C3%ADa-En-Colombia-Se-Presentan-Cerca-de-79-Casos-de-Violacion-de-Proteccion-de-Datos-Personales

Welivesecurity. (2021). *Venden datos de 1.500 millones de usuarios de Facebook recopilados mediante scraping*. Https://Www.Welivesecurity.Com/La-Es/2021/10/05/Venden-Datos-1-500-Millones-Usuarios-Facebook-Recopilados-Mediante-Scraping/