Desafíos constitucionales de la privacidad en la era digital: la eficacia del derecho público en la protección de datos personales[1]

Constitutional challenges to privacy in the digital age: The effectiveness of public law in the protection of personal data

Rafael Calderón[2]

Mario Federico Pinedo[3]

Resumen: este artículo analiza el marco legal colombiano encargado de garantizar el derecho a la protección de información y la privacidad bajo la difusión no autorizada de materiales e información privada en la era digital. Para ello, se estudia en base a los objetivos de: 1) evaluar la efectividad de las leyes vigentes y su implementación práctica y 2) proponer reformas específicas para fortalecer el marco legal del derecho a la privacidad. Se opta por un enfoque cualitativo, con una fase exploratoria-descriptiva y una expositiva-comparativa, en las que se evalúan el artículo 15, la Ley 1266 de 2008 y la Ley 1581 de 2012, con el objeto de comparar las legislaciones internacionales. A modo de conclusión, este trabajo subraya la importancia de la educación ciudadana sobre la privacidad digital y la urgencia de fortalecer las leyes en Colombia que la garanticen.

Palabras clave: protección de datos personales, derecho a la privacidad, normativa constitucional, consentimiento informado.

---

[1] Artículo científico presentado como opción de grado para optar por el título de Magíster en Derecho Público.

[2] Abogado egresado de la Universidad Santo Tomás. Magíster en Derecho Administrativo de la Universidad Sergio Arboleda. Especialista en Derecho Administrativo, Derecho Minero Energético y Contratación Estatal. Rafael.calderon84@hotmail.com

[3] Magíster en Derecho Público de la Universidad Santo Tomás (Bogotá). Especialista en Derecho Administrativo, abogado. Docente de la Universidad Santo Tomás, Bogotá. https://1bestlinks.net/LnMCz - https://1bestlinks.net/eNQfe- https://lbestlinks.net/WxcyU. mfedericopinedom@gmail.com

Abstract: This article analyzes the Colombian legal framework in charge of guaranteeing the right to the protection of information and privacy under the unauthorized dissemination of materials and private information in the digital era. For this purpose, it is studied based on the objectives of: 1) evaluating the effectiveness of current laws and their practical implementation and 2) proposing specific reforms to strengthen the legal framework of the right to privacy. A qualitative approach is chosen, with an exploratory-descriptive and an expository-comparative phase, in which Article 15, Law 1266 of 2008 and Law 1581 of 2012 are evaluated, in order to compare international legislations. By way of conclusion, this work underlines the importance of citizen education on digital privacy and the urgency of strengthening the laws in Colombia that guarantee it.

Keywords: Protection of Personal Data, right to privacy, constitutional norms, informed consent.

I. Introducción

Históricamente, la privacidad ha sido reconocida como ley constitucional de carácter fundamental, cuya evidencia se encuentra en las primeras constituciones y declaraciones de derechos y, posteriormente, en tratados internacionales y constituciones contemporáneas. Con el avance de las Tecnologías de la Información y las Comunicaciones (TIC) en el siglo XXI ha incrementado la conciencia y la regulación en torno a la privacidad. Sin embargo, la era digital y el auge de la globalización han transformado este panorama, en la medida en que las sociedades se enfrentan a una amenaza latente en términos de privacidad, debido a la vulnerabilidad de la protección de informaciones personales.

Aunque el artículo 15 de la Constitución Política defina la protección de lo privado bajo el siguiente estatuto: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar" (Constitución Política de Colombia [C.P.], 1991, art. 15), la naturaleza ubicua de la tecnología digital hace de la protección a la privacidad un desafío continuo y complejo, haciendo necesaria la actualización constante de los marcos constitucionales, tanto así que se estima necesario la creación de leyes adecuadas que puedan aplicarse efectivamente en un entorno cambiante.

Siguiendo esta idea , el crecimiento de la recolección masiva de datos y las prácticas comunes de difusión no autorizada de material privado generan hoy en día conflictos significativos que incluyen el desconocimiento del consentimiento informado, el uso indebido de la información personal, la vigilancia masiva, las amenazas a la ciberseguridad[4] y un sin fin de otros elementos que amenazan la vida digna. Es decir que, aunque existe un marco legal-normativo –que incluye, pero no termina con el artículo mencionado–, los desafíos para la buscar una protección principalmente eficaz del derecho a la privacidad en la era digital siguen siendo numerosos.

En relación con esta problemática, es fundamental destacar el papel de la jurisprudencia de la Corte Constitucional de Colombia en la interpretación y aplicación de normas, al destacar la importancia de asegurar una igualdad equilibrada entre proteger la privacidad y otros intereses públicos como la seguridad y la justicia. No obstante, la legislación colombiana sigue sin ser suficiente hacer valer eficazmente la privacidad como

[4] Sobre la ciberseguridad en el trabajo de grado *Política criminal del delito informático en Colombia*, Carreño y Baquero (2023). Mencionan que "de los delitos más frecuentes, constituidos en forma de mercado en el contexto internacional de la Deep Web, están conformados por la venta de datos" (p.10). Para ampliar información sobre este asunto, revise el enlace: http://hdl.handle.net/11634/50772

derecho frente a la difusión no autorizada de material privado en la era digital. Por consiguiente, esto continúa representando un desafío para el país a causa de la deficiente adaptación de este marco legal a las nuevas tecnologías y la garantía de los derechos fundamentales en este contexto. De lo anterior, surge la importancia de construir y responder la pregunta de investigación: ¿De qué manera se puede fortalecer la Constitución Política colombiana y su marco jurídico que garantice efectivamente el derecho a la privacidad frente a la difusión no autorizada de material privado en la era digital?

La salvaguarda de este derecho en la era digital ha despertado un interés creciente en el sector legal y académico. Por ello, se revisan a continuación los antecedentes relacionados con el problema jurídico en relación al tema central, con el objetivo de comprender su contexto y las relaciones temáticas preexistentes a la protección de este. En conformidad con lo señalado, se realizó un mapeo exhaustivo de las investigaciones, cuya genealogía reveló una evolución significativa en el tratamiento de la privacidad en línea y la difusión no autorizada de material privado. Ahora bien, se encontró que los estudios han abordado esta cuestión desde diferentes perspectivas, al examinar tanto el marco legal existente como los desafíos y oportunidades que plantea el entorno digital.

En primer lugar, el trabajo investigativo de Riesco (2022) tuvo el objetivo de examinar el impacto de la tecnología en la libertad de expresión y la privacidad, al destacar la necesidad de proteger estas garantías en un mundo cada vez más digitalizado. Asimismo, este autor definió y comprendió estos derechos al abordar sus evoluciones históricas y jurídicas, así como los límites surgidos con los desafíos actuales. Por tal motivo, el autor señaló que “[...] la intimidad es una parte clave en la formación de la doctrina del derecho a la protección de datos personales, y se ponen en conexión en tanto que este último debe de

entenderse como un control de información personal" (p. 41), con la finalidad de salvaguardar la integridad de los individuos.

Seguidamente, el artículo de Orfale (2020) analizó la Ley 1962 de 2019, la cual establece un marco normativo para la creación, organización y funcionamiento de las regiones en Colombia. En vista de lo anterior, en este trabajo se revisaron los antecedentes históricos que llevaron a la existencia de esta ley y se destacaron aspectos clave como la descentralización, la autonomía regional, la creación de órganos de Gobierno y la distribución de competencias entre los niveles gubernamentales para representar los intereses locales. Teniendo en cuenta lo anterior, se concluyó que esta ley promueve una mayor equidad territorial y una mejor distribución de recursos en Colombia.

Por otro lado, desde un enfoque más sistémico se hizo un rastreo de los estudios realizados en la Universidad Santo Tomás, localizando investigaciones[5] (Arévalo, 2020), donde se expone la utilización de datos personales en el mundo digital, como la moneda emergente del siglo XXI, que ha orientado la orientación de las normativas estatales para garantizar una salvaguarda adecuada de los datos personales durante su procesamiento. En esta investigación, se examinó el impacto del Tratamiento de Datos Personales (TDP) en el derecho al habeas data y la manera en que la ley colombiana actúa para alcanzar un nivel de TDP conforme a las normas internacionales.

En este mismo sentido, se identificaron investigaciones[6] (Galvis, 2012), que analizaron los progresos y desafíos de Colombia frente a la protección de datos personales.

[5] *Protección de datos personales en Colombia frente al profiling y entornos digitales* (2020). Tesis de grado. Universidad Santo Tomás.

[6] *Protección de datos en Colombia, avances y retos* (2012). Artículo resultado parcial de la investigación doctoral sobre protección de datos personales que la autora realiza en el Doctorado de la Facultad de Derecho, Universidad Santo Tomás (Colombia).

Para ello, se tuvo en cuenta la seguridad jurídica y los derechos fundamentales como el *habeas data*, la intimidad, la honra, el buen nombre, la información y la libertad informática, en el marco de las tecnologías emergentes y las exigencias internacionales. Además, se analizó la legislación relativa a la salvaguarda de la información personal y su relación con la Responsabilidad Social Empresarial.

De la misma manera, se encontró un estudio de Peña[7] (2018) que evaluó los aspectos significativos de los aspectos legales sobre la protección de datos personales en el contexto nacional e internacional, lo que proporcionó un marco normativo comparativo. La autora enfocó el estudio en el envío y recepción de datos de forma internacional perteneciente a ciudadanos y enviados a otros países, el cual debe regularse por las leyes colombianas.

Por otro lado, el trabajo enfocado en este derecho en Colombia, Valencia[8] (2016) definió la intimidad como una característica esencial del ser humano que depende de la madurez emocional y la protección jurídica disponible en un momento dado. Esto destaca su protección dentro del ámbito familiar e individual, al asegurar la reserva y confidencialidad de estas. Dicho lo anterior, la presente investigación tuvo en cuenta estudios de la misma fuente, debido a que enriquecen el fundamento investigativo de este trabajo.

Los estudios señalados son solo una parte de la amplia variedad de temas relacionados que se han tratado en relación con la protección de la privacidad, incluyendo la regulación del uso de datos personales, la privacidad en las redes sociales y los desafíos éticos y legales

---

[7] *Retos regulatorios de la protección de datos en Colombia* (2018). Tesis de maestría. Universidad Santo Tomás.

[8] *El derecho fundamental a la intimidad en el contexto digital de Colombia* (2016). Disertación doctoral. Universidad Santo Tomás.

asociados con la difusión no consentida de información privada. Como resultado, la revisión de antecedentes reveló que aún quedan interrogantes por abordar y desafíos por superar para garantizar una protección efectiva de los derechos individuales en esta contemporaneidad mediada por los avances tecnológicos.

En conformidad con lo expuesto, este artículo tuvo el fin de analizar el marco legal colombiano encargado de proteger el derecho a la privacidad frente a la difusión no autorizada de materiales y datos privados en la era digital, al considerar las múltiples lagunas en la normativa actual y la propuesta de reformas para mejores prácticas. Para el desarrollo de este planteamiento, los objetivos específicos fueron: 1) evaluar la efectividad de las disposiciones legales vigentes para abordar la difusión no autorizada de materiales y datos privados en el contexto digital, destacando los desafíos y obstáculos en su implementación práctica; y 2) proponer reformas específicas para fortalecer el marco legal colombiano y mejorar la protección del derecho a la privacidad, al incorporar mejores prácticas nacionales e internacionales y garantizando un equilibrio adecuado entre la privacidad y otros intereses públicos.

Para alcanzar los objetivos planteados, este artículo se dividió en tres apartados. En primer lugar, se definen las nociones conceptuales centrales para el abordaje del estudio; en segundo lugar, se expone la metodología de análisis y las fases en que se llevó a cabo el estudio del marco legal colombiano vigente en función de la protección de la privacidad de datos personales en contraste con la normativa internacional. Finalmente, se exponen los resultados de la actividad comparativa y las conclusiones encaminadas a propuestas de reforma a la normativa legal de Colombia, con la finalidad de asegurar y preservar políticas de protección de datos de los ciudadanos.

II. Funcionalismo y privacidad de datos personales: una aproximación conceptual

Con el fin de sustentar este trabajo, se recurrió a la aplicación de la teoría del funcionalismo, centrada en el análisis de las funciones que cumplen las instituciones en el ámbito legal, como normas y prácticas jurídicas en la sociedad. En efecto, este enfoque teórico evalúa si dichas funciones contribuyen al bienestar general, la estabilidad social y la eficiencia del sistema legal. Por lo tanto, al aplicar el funcionalismo al derecho se busca comprender cómo las diferentes partes del sistema legal interactúan para lograr objetivos específicos. Ahora bien, en el contexto de la era digital, es necesario reconocer cómo estas normas e instituciones velan por la integridad individual y colectiva.

En ese orden de ideas, el estudio del funcionalismo estructuralista propuesto por Parson sostiene que las leyes y las normas funcionan en función de su contexto y realidad. De acuerdo con Montero en su artículo online (2008):

> [...] el funcionalismo estructural o estructural-funcionalismo, enfatiza la relación entre las funciones y las partes del todo que las desarrolla. Estudia la sociedad misma, considerada en su globalidad, para buscar las funciones esenciales que deben ser desempeñadas por individuos, grupos o instituciones, para que la sociedad se configure y perdure.

Como contraposición, es importante señalar que el funcionalismo ha sido objeto de críticas por varios motivos. En primer lugar, se argumenta que tiende a justificar el *status quo* y puede ser reacio a promover cambios radicales en el sistema legal. Aunado a esto, algunos críticos señalan que asume que todas las partes del sistema legal deben tener una función positiva, lo que ignora la posibilidad de disfunciones y conflictos internos. Por otro

lado, puede simplificar excesivamente las complejas interacciones entre las normas legales y la sociedad, obviando factores contextuales y culturales.

Sin embargo, su importancia en este estudio y en futuros esfuerzos dentro de este contexto, se basa en la imperiosa necesidad de ajustar las normativas de salvaguarda de datos personales a los retos de la era digital, considerando que la privacidad es un derecho esencial que debe ser resguardado de manera eficiente en un contexto donde la información personal está expuesta a diversas amenazas tecnológicas.

De acuerdo con lo planteado, se retomó el interrogante de la presente investigación para dar respuesta y sustentar la hipótesis. Por tal razón, se identificaron y definieron los conceptos esenciales del estudio, los cuales se aplicaron para resolver el problema de la protección del derecho a la privacidad en la era digital en Colombia.

En primer lugar, el derecho a la privacidad se define como la capacidad de los individuos para controlar la información sobre sí mismos y proteger su vida personal, familiar y comunicaciones de intrusiones no autorizadas. Al respecto, Moreno y Olmeda (2021) ampliaron esta definición al reconocer que este es un derecho fundamental que protege aspectos como la inviolabilidad del domicilio y la confidencialidad de la correspondencia. Por su parte, Pfeiffer (2008), citando a Sennet (1978), reconoció como privacidad lo siguiente:

> [...] todo lo que está fuera del ámbito del interés público, de los asuntos del Estado, de lo que involucra al conjunto de la sociedad. Lo privado es el ámbito restringido de lo doméstico y lo familiar, de aquellos asuntos del sujeto, que no necesariamente deben divulgarse masivamente. Esto es precisamente lo que dificulta la vida en

> comunidad y lo que exige soluciones políticas a los conflictos inevitables. (pp. 14-15)

Otro concepto relevante es la salvaguarda de la información personal, también denominada habeas data. Este es un derecho esencial que otorga a las personas la posibilidad de conocer, actualizar y rectificar los datos recabados sobre ellas en bancos de datos y archivos de organismos públicos y particulares. Gregorio (2005), en su definición, la describió como un conjunto de reglas y principios que regulan la recopilación, el manejo, el almacenamiento y la divulgación de datos personales, con el objetivo de asegurar que las personas mantengan el control de sus datos.

Según la investigación realizada en la Unidad de Planeación Minero-Energética [UPME] (2021), la protección de datos personales se reconoce como un derecho:

> Derecho fundamental, en virtud del cual las personas gozan de garantías en relación con su intimidad personal y familiar y su buen nombre [...] Este derecho es comúnmente conocido como habeas data, y si bien está catalogado como garantía constitucional autónoma, está vinculado con los derechos a la honra, la intimidad, la reputación, el libre desarrollo de la personalidad y el buen nombre. (p. 1)

En tercer lugar, el consentimiento en el derecho es la manera de permitir algo o de mostrarse de acuerdo con la voluntad, ideas u opiniones de otra persona. Por consiguiente, el consentimiento informado es un principio relevante en la protección de datos personales, que requiere que los individuos sean plenamente informados sobre cómo se recolectarán, usarán y compartirán sus datos antes de dar su consentimiento, al asegurar que este sea libre y consciente (Franco, 2005; Berro, 2013).

Finalmente, la vigilancia masiva se refiere al monitoreo extensivo y sistemático de las actividades de grandes grupos de personas, mediante tecnologías avanzadas como cámaras de seguridad, software de reconocimiento facial y monitoreo de actividades en línea. En conformidad con Salamanca (2014) y Serra (2015), la vigilancia masiva implica la recolección de datos personales sin un enfoque específico, incluyendo la interceptación de comunicaciones y la recopilación de datos de ubicación.

En resumen, como se mencionó, estas nociones conceptuales son esenciales para abordar la problemática sobre el derecho a la privacidad en la era digital en Colombia. Se podría argüir que este marco proporciona una base sólida que orienta la investigación hacia la identificación de debilidades en la legislación actual, lo que permite proponer reformas y mecanismos efectivos que mejoren la protección de la privacidad y, por consiguiente, salvaguarden el cumplimiento del derecho de los ciudadanos en el contexto de las tecnologías digitales.

2.1 Normativa colombiana e internacional: fases del estudio

Esta investigación empleó un enfoque metodológico cualitativo, el cual se llevó a cabo en tres fases. En la primera fase, denominada exploratoria-descriptiva, se realizó una revisión bibliográfica y documental exhaustiva sobre las disposiciones actuales ofrecidas por la Constitución Política colombiana en materia de protección a la privacidad y a los datos personales. Esto implicó el análisis del marco legal-normativo del país, con especial atención al artículo 15 y a leyes complementarias como la 1266 de 2008, o Ley de *habeas data*, y la 1581 de 2012, o Ley de Protección de Datos Personales).

Además, se examinaron las sentencias clave de la Corte Constitucional: T-280 de 2022 y T-339 de 2022. Aunado a esto, esta revisión se acompañó de casos prácticos para evaluar la aplicabilidad y la efectividad del marco legal. Por lo tanto, se seleccionaron casos emblemáticos en los que se haya vulnerado el derecho a la privacidad. Finalmente, se realizó un análisis detallado de los procedimientos judiciales y las resoluciones emitidas, con el fin de identificar patrones y desafíos comunes en la implementación de la legislación.

En una segunda fase, denominada expositiva-comparativa, se estudiaron, de manera detallada, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (UE) y las legislaciones de países latinoamericanos como México y Argentina, para conocer las estrategias y normativas en relación con la protección de datos privados en estos marcos internacionales. Ahora bien, estas dos fases iniciales tuvieron como objetivo identificar las falencias y vacíos existentes en las disposiciones colombianas, en contraste con mejores prácticas internacionales en términos de prevención y protección de derechos fundamentales como el de la privacidad e intimidad.

Lo mencionado dio lugar a una tercera y última fase, en la que se desarrollaron propuestas de reforma adaptadas al contexto colombiano que buscan garantizar una protección robusta de la privacidad en la era digital. Asimismo, se evaluó el impacto potencial de las reformas propuestas y se promoverán programas de educación sobre privacidad digital, con el fin de sensibilizar a la población sobre la importancia de la privacidad bajo este contexto mediado por los avances tecnológicos. Igualmente, se elaboraron medidas de evaluación y monitoreo para asegurar la efectividad de las reformas, en consonancia con iniciativas educativas que fomenten una cultura de respeto y de protección a la privacidad. En otras palabras, las fases establecidas para esta investigación

permiten un abordaje integral y sistemático del problema, con la finalidad de identificar y solucionar las lagunas actuales en el marco legal colombiano, así como proponer reformas efectivas para reforzar e intensificar la protección del derecho a la privacidad en la era digital.

La privacidad y el tratamiento de información dentro de la esfera constitucional

Artículo 15

El artículo 15 de la Constitución Política de Colombia establece lo siguiente:

> [...] Tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden interceptarse o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. (Constitución política de Colombia [C.P.], 1991, art. 15).

A través de este artículo se garantiza el derecho a la privacidad de los ciudadanos, los cuales tienen la autonomía de decidir, actualizar y corregir la información que suministren a entidades ajenas. Es decir, pueden solicitar o exigir que la recolección, tratamiento y circulación de sus datos sean manejados bajo confidencialidad y reserva. En caso de que esto sea violado, el Estado está en la obligación de intervenir y sancionar.

Indudablemente, con la proliferación de las nuevas tecnologías, numerosas empresas recolectan datos a través de medios digitales, lo que puede representar una amenaza hacia la privacidad de las comunicaciones electrónicas, las redes sociales y las conversaciones telefónicas sobre la información médica y financiera de los ciudadanos, así como en casos de vigilancia estatal y actividades de recolección de datos por parte de entidades privadas.

Frente a esto, el artículo 15 garantiza la protección de los datos personales, lo que es fundamental en una sociedad democrática y respetuosa de los derechos individuales. En este sentido, y teniendo en cuenta el enfoque tecnológico, resulta crucial que las leyes y políticas relacionadas con la protección de la privacidad se actualicen para abordar los riesgos y preocupaciones asociadas con la tecnología moderna. En consecuencia, esto podría implicar el desarrollo de regulaciones específicas sobre el uso de datos personales en línea, la implementación de medidas de seguridad cibernética para proteger la información privada y la promoción de la educación digital para concienciar a los ciudadanos sobre sus derechos de privacidad en el mundo digital.

En concordancia con lo expuesto, Ayala et al. (2020) afirmaron que, gracias a la evolución de la tecnología, que es acelerada y desenfrenada, se han derivado nuevos retos en función de los datos personales y su recolección, almacenamiento y tratamiento a través de diferentes medios digitales y tecnológicos[9]. Por lo general, esta actividad se ha relacionado con fines comerciales. En épocas antiguas, según estos autores, en temas de hacienda pública los gobernantes reconocían la necesidad de realizar el debido tratamiento de los datos para verificar responsabilidades tributarias. En contraste, se encuentra la siguiente observación:

> Al transcurrir el tiempo, el ya mencionado desarrollo tecnológico, causó que la "simpleza" que se tenía antes frente al manejo de datos cambiara su curso, pues se evidenció la necesidad de que el manejo de estos llevara consigo un proceso debido,

[9] Los autores, citando a Recio (2019), mencionan que el "crecimiento en el manejo de información se encuentra estrechamente relacionado con los diferentes medios tecnológicos que se utilizan para hacer posible la divulgación masiva de los datos; en el año 2018 se estimaba una cantidad de 23.14 billones de dispositivos digitales que hacían uso a plataformas como internet, de esta cantidad de dispositivos llama la atención que resulta ser más elevada que la cantidad de usuarios que se registran, pues para el mismo año se estimaba un total de 3.9 billones de usuarios conectados" (p. 8).

> motivo por el cual las plataformas digitales se vieron en la obligación de dar la respectiva protección de datos, garantizando que los requerimientos legales quedarán resueltos. (Ayala et al., 2020, p. 8)

En ese sentido, se demuestra que la acumulación de datos personales se ha respaldado durante años por el desarrollo normativo, de manera que, a nivel nacional, se ha creado un marco legal que aborda los desafíos de la digitalización. Estas normativas no solo protegen los derechos de los individuos, sino que también fomentan un entorno de confianza y responsabilidad, lo cual es crucial para el crecimiento sostenible de la economía digital. En conjunto, la combinación de herramientas tecnológicas avanzadas y un sólido marco normativo permite enfrentar los desafíos emergentes de lo digital, al equilibrar la innovación tecnológica con la protección de derechos fundamentales.

Frente a este panorama surgió la necesidad de constituir estrategias o lineamientos generales fundamentados en la legalidad para garantizar y asegurar la privacidad de las personas en la era digital. Como ejemplo de esto se encuentran los siguientes principios: el principio de finalidad del tratamiento, el principio de proporcionalidad y el principio de minimización de datos[10]. En el caso particular de Colombia, se procuró la elaboración de un marco jurídico que fuese capaz de regular y velar por el tratamiento adecuado de la información suministrada por los ciudadanos con el objetivo de proteger la integridad.

[10] Para ampliar la información relacionada a los principios sobre la privacidad y protección de datos personales se invita a revisar el informe de la Organización de los Estados Americanos (OEA) disponible en el siguiente enlace: https://www.oas.org/es/sla/cji/informes_culminados_recientemente_Proteccion_Datos_Personales.asp

Si bien este tuvo su inicio con el artículo 15 de la Constitución de 1991, posteriormente se expidió la Ley 1266 de 2008[11] que abordó de manera limitada el tratamiento de datos personales solo en relación con la vida crediticia de los individuos. No obstante, esta problemática halla finalmente su fundamentación normativa principal en la Ley 1581 del 2012 y será a partir de esta que se desarrolle el debate y las actualizaciones hasta el día de hoy. A continuación, se expondrá este recorrido normativo, el cual se acompañó de los casos prácticos correspondientes que dieron origen a cada disposición.

Ley 1581 de 2012

La Ley 1581 de 2012, también llamada Ley de Protección de Datos Personales en Colombia, rige la recopilación, el almacenaje, el empleo, el flujo y la eliminación de datos personales proporcionados en bases de datos o archivos. Sin embargo, el propósito de esta es asegurar y salvaguardar los derechos esenciales de la privacidad y el buen nombre, garantizando que la gestión de los datos personales se lleve a cabo con total consideración a los derechos de los propietarios de la información.

Esta normativa también protege otros derechos, libertades y salvaguardas constitucionales vinculados con la privacidad y la salvaguarda de la información personal. De acuerdo con la Constitución Política, la Ley 1581 dicta un conjunto de principios y responsabilidades para las instituciones que gestionan datos personales, garantizando que el

[11] Sobre esta ley, Ayala et al. (2020) mencionaron que "son claras las intenciones que tuvo el legislador al expedir la Ley 1266 de 2008 para tratar de regular aspectos relacionados con el manejo de datos personales, no obstante, es notorio que la misma se centró en el manejo de datos de carácter crediticio y financiero, en razón a esto no consigue cubrir los aspectos generales de tratamiento de datos personales, generando vacíos normativos que promovían la propagación de problemas frente al manejo de datos en entidades públicas y privadas, provocando así la necesidad de cubrir normativamente aspectos con relación al tema, a fin de incluir y salvaguardar de manera integral todo el tratamiento de datos en Colombia" (p. 11). La discusión completa fue arrojada del siguiente enlace: http://hdl.handle.net/10823/2142

manejo de dicha información se lleve a cabo de forma transparente y segura respetando los derechos de las personas.

Asimismo, entre sus disposiciones, la ley establece el consentimiento informado como un requisito esencial, lo que promueve la autonomía y el control de los ciudadanos sobre su información (Baquero, 2015). Además, crea mecanismos para la protección de datos, incluyendo la figura del "responsable" y del "encargado del tratamiento", quienes deben garantizar el cumplimiento de las normas de protección. De igual modo, establece sanciones para las entidades, lo que refleja un compromiso claro con la defensa de los derechos individuales en la era digital (Congreso de la República, Ley 1581/12).

Por ejemplo, en 2013, la Superintendencia de Industria y Comercio (SIC) descubrió que Bel-Star S.A., una compañía dedicada al diseño, fabricación y comercialización de productos cosméticos, a través de la venta directa y parte estratégica de la Corporación Belcorp, estaba violando la obligación legal de notificar previamente a los ciudadanos que serían reportados en las centrales de riesgo[12]. Al respecto, esta notificación previa es crucial para que los ciudadanos puedan pagar su deuda pendiente o disputarla antes de exponerse a dicho reporte. Como resultado de esta infracción, la SIC impuso a Bel-Star S.A. una sanción de COP 235 800 000; además, le ordenó a la entidad que se eliminaran de las historias de crédito los reportes negativos en los casos donde no se cumplió con la comunicación previa obligatoria. Durante la investigación, la SIC también encontró que los cobradores

[12] El reportaje indicó como la empresa se encontraba utilizando los datos de sus clientes con el fin del manejo de estos (Mancera, 2013). puede encontrar el Reportaje completo en el siguiente enlace: https://www.asuntoslegales.com.co/actualidad/confirman-sancion-a-bel-star-por-violar-habeas-data-2041886

prejurídicos de Bel-Star S.A. daban a los deudores plazos inadecuados, a veces de solo días u horas, para ponerse al día con sus obligaciones en mora.

Es crucial señalar que la SIC posee el poder de aplicar sanciones de hasta mil quinientos salarios mínimos legales mensuales actuales (1.500 SMLMV) por infracciones a la Ley 1266 de 2008, y de hasta dos mil salarios mínimos legales mensuales actuales (2.000 SMLMV) por transgresiones a la Ley 1581 de 2012. Asimismo, puede solicitar la interrupción de actividades o la clausura temporal o definitiva de operaciones vinculadas con el manejo de información personal.

Sentencia T-280 de 2022

La Sentencia T-280/22 de la Corte Constitucional aborda cuestiones relacionadas con el derecho a la intimidad y a la imagen. Sobre esto, es importante señalar que esta sentencia se originó por el caso de la grabación y divulgación no consentida de las imágenes de una mujer mientras realizaba actividades fisiológicas; la escuela en la que se presentaron los hechos permitió esta actividad, incumpliendo sus deberes de diligencia y vulnerando el derecho a la intimidad.

En consecuencia, el dictamen de la sentencia destacó que este derecho ha evolucionado hacia una concepción amplia y social, proyectándose en lugares públicos y privados debido a la expectativa razonable de intimidad en ambos contextos. La grabación subrepticia de la imagen evidencia una intención de evadir el consentimiento y de usar el material sin autorización. Adicionalmente, la divulgación no consentida del video se consideró una forma de violencia de género en línea. Lo anterior exhortó al Congreso, ante la falta de una ley específica para abordar la violencia digital contra las mujeres, a legislar

sobre esta e instó a la toma de medidas urgentes y coordinadas entre autoridades con una perspectiva de género.

En cuanto a la respuesta legal del caso, la Corte ordenó medidas para proteger los datos personales, incluyendo la eliminación del contenido dañino y el cese de su distribución. Asimismo, enfatizó en la necesidad de colaborar activamente en la denuncia y prevención de este tipo de violencia.

Antes de la creación de dicha sentencia, la cual se convirtió en una alternativa para brindar solución a situaciones que ponen en riesgo la integridad y los derechos fundamentales de las mujeres, se presentó ante la Corte Constitucional de Colombia el caso de una mujer[13] que experimentó la difusión no consensuada de fotos íntimas en plataformas como Facebook y WhatsApp, lo que generó un impacto psicológico, emocional y físico significativo en ella.

En esa medida, la demandante, al recurrir a una acción de tutela, solicitó la eliminación de las publicaciones, disculpas públicas y medidas disciplinarias contra la responsable, entre otras acciones. Bajo este escenario, la Corte reconoció el daño más allá de la eliminación de las publicaciones, al destacar el poder ejercido sobre la víctima por aquellos que poseen y amenazan con divulgar las imágenes íntimas. Sin embargo, esta sentencia se cuestionó por no tener un abordaje desde un enfoque de género. En consecuencia, la solución de la Corte se centró solo en la protección de datos, ignorando el impacto de la difusión de imágenes íntimas y la violencia en línea[14].

[13] Sentencia del 13 de enero de 2021. Esta puede consultarse como Sentencia T-339/22.

[14] Esta sentencia tuvo un proceso de revisión de los fallos anteriores, lo que dio lugar a la Sentencia T-339/22, en la que se aplicaron nuevas consideraciones sobre la publicación de imágenes sin consentimiento. Concluyendo sobre la vulnerabilidad del derecho a la intimidad y al manejo de la propia imagen.

A modo de corolario, los dos casos presentados, con sus respectivas sentencias, ponen de relieve la urgencia de formular y llevar a cabo acciones para salvaguardar el derecho a la intimidad y la protección de datos privados, puesto que la circulación de estos últimos, sin consentimiento, puede afectar la salud mental y física de la víctima, lo que atenta contra varios de sus derechos fundamentales, constituyendo así una forma de violencia.

Ley 1266 de 2008

La Ley 1266 de 2008, también denominada Ley *habeas data,* controla la gestión de los datos presentes en las bases de datos personales colombianas. Su meta principal se enfoca en fomentar el derecho constitucional de los individuos a conocer, renovar y rectificar la información recolectada sobre ellos en bancos de datos, poniendo especial atención en la información financiera, crediticia, comercial, de servicios y procedente de terceros países. En resumen, este reglamento tiene como objetivo asegurar los derechos vinculados con la recopilación, el manejo y la circulación de información personal[15] con el derecho a la información[16] establecido en la Constitución Política.

Si bien la Ley *habeas data* se aplica a todos los datos de información personal registrados en bancos de datos administrados por entidades públicas o privadas, presenta algunas excepciones como las bases de datos del Departamento Administrativo de Seguridad (DAS) y de la Fuerza Pública para garantizar la seguridad nacional interna y externa, así como los datos exclusivamente personales, domésticos o de circulación interna (Ley 1266, 2008). En suma, esta ley es fundamental para proteger los derechos de privacidad y del

[15] Información extraída del Artículo 15 de la Constitución Política de Colombia.
[16] Información extraída del Artículo 20 de la constitución política de Colombia.

control y tratamiento de la información de datos suministrada por los ciudadanos colombianos.

Las normativas presentadas hasta el momento permiten comprender el funcionamiento del marco jurídico colombiano dentro del plano de la privacidad en el tratamiento de datos o difusión de contenidos privados. A partir de lo anterior, se puede asegurar que existen otras leyes y normas que permiten continuar construyendo este marco. No obstante, algunas de estas se encuentran obsoletas, como el artículo 15. Como consecuencia, nace la necesidad de reestructurarlas para obtener una mejora en los resultados de estudio. Por tal razón, la normativa legal se debe actualizar conforme a los avances tecnológicos, cuya idea se sustentó bajo la mención realizada por el presidente de Asobancaria, José Manuel Gómez, quien expresó lo siguiente:

> En este sector se ha hecho mucho por el esquema de responsabilidad demostrada, ya que obliga a ser mucho más proactivos en el manejo de la información, pero lo más grave es que con el desarrollo tecnológico esto no termina, ya que este va introduciendo nuevos esquemas de manejo de la información, donde la responsabilidad implica que se tiene que implementar un esquema nuevo para esas nuevas tecnologías de la información, donde en 10 años va a ser distinto a como se maneja hoy, pero siempre implementando políticas, procedimientos, capacitaciones y un equipo que maneje la información al interior de las de las entidades. (Gómez, 2022, como se citó en Quiñones, 2022, p. 25)

Al respecto, es pertinente señalar que, en caso de que las leyes no evolucionen en concordancia con su contexto, pueden surgir lagunas y dificultades que complicarían la compresión e interpretación de estas dentro del ámbito jurídico y legal. Respecto a esto,

muchos países extranjeros han implementado medidas para manejar las políticas de tratamiento de datos.

2.2 Actividad comparativa

2.2.1 Reglamento General de Protección de Datos de la Unión Europea

El GDPR es un reglamento de la Unión Europea que se implementó en mayo de 2018, que dicta las directrices sobre cómo las compañías y otras entidades deben manejar los datos personales de los ciudadanos de esta comunidad política-democrática. Según Piñar (2022), el objetivo principal del GDPR es robustecer y homogeneizar la salvaguarda de datos para todos los individuos dentro de la UE, así como regular la transmisión de datos personales más allá de ella. Se ha establecido que una de sus estipulaciones más relevantes es la demanda del permiso de las personas frente a las compañías para el manejo de sus datos personales. Asimismo, el GDPR concede a los usuarios un conjunto de derechos que comprenden: el derecho de acceso, de rectificación, de supresión y de restricción del procesamiento. Además, establece la responsabilidad y la rendición de cuentas, junto con la comunicación de infracciones de datos y la penalización de estas medidas (Piñar, 2022).

En resumen, el GDPR es una ley rigurosa y sólida destinada a salvaguardar la privacidad y los derechos de las personas en el ámbito digital, ya que impone normas altas para el manejo de datos personales y fomenta la transparencia y la responsabilidad de las entidades que manejan estos datos. Para Colombia, las leyes deben ser ligeramente más estrictas para garantizar que las compañías honren la integridad de cada persona.

2.3 Legislaciones de México y Argentina

En México, la salvaguarda de los datos personales se rige por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dictada el 26 de enero de 2017 y puesta en circulación en el Diario Oficial del Estado. De acuerdo con la Cámara de Diputados, esta normativa de orden público y vigente en todo el territorio mexicano define los principios, fundamentos y procedimientos requeridos para proteger el derecho de los individuos a la salvaguarda de sus datos personales. Como resultado, los individuos sujetos a esta normativa comprenden autoridades, entidades, órganos y entidades de los poderes Ejecutivo, Legislativo y Judicial, además de partidos políticos, fideicomisos y fondos públicos. Finalmente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) iene la responsabilidad de supervisar y aplicar esta ley (Cámara de Diputados, 2017).

De igual forma, en Argentina, la salvaguarda de la información personal es un derecho constitucional establecido desde la reforma de 1994. Así, la Ley 25.326, establecida en la nación, define los principios, derechos y responsabilidades para el manejo correcto de la información personal, con el objetivo de proteger la privacidad y la seguridad de dichos datos (Consejo general de la transparencia, 2022). Sin embargo, esta normativa impide concretamente el empleo de datos para propósitos diferentes a los que se recogieron; de esta forma, se garantiza el resguardo de la privacidad de las personas. La responsabilidad de supervisar y regular la implementación de esta regulación en Argentina recae en la Agencia de Acceso a la Información Pública (AAIP).

Al considerar el breve recorrido sobre las protecciones al derecho de la privacidad condensadas en el GDPR y en las legislaciones de México y Argentina, se presenta un cuadro comparativo que tiene como objetivo servir de modelo o referente normativo para su aplicación en el marco regulatorio de Colombia. Los criterios comparativos seleccionados para ello son los siguientes: *objeto* y *principios fundamentales.*

Tabla 1. *Normativa internacional sobre protección de datos personales (UE, México, Argentina).*

Lugar de legislación	Norma	Objeto	Principios fundamentales
Unión Europea	**Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo** de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)	Las reglas y principios relacionados con la protección de las personas físicas en relación con el manejo de sus datos personales deben, sin importar su nacionalidad o lugar de residencia, salvaguardar sus libertades y derechos esenciales, especialmente el derecho a la salvaguarda de los datos personales.	Licitud y transparencia Integridad y confidencialidad Exactitud Finalidad y limitación de plazo de conservación
México	**Ley general de protección de datos personales en posesión de sujetos obligados** (Texto Nueva Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017)	El objetivo es definir los fundamentos, principios y procesos para asegurar el derecho de cada individuo a la protección de sus datos personales, en manos de entidades obligadas.	Consentimiento Exactitud Transparencia Veracidad o calidad de los registros o datos
Argentina	**Protección de Datos Personales Ley 25.326** Disposiciones Generales. Principios generales	La finalidad de esta ley es salvaguardar de manera integral los datos personales contenidos en	Licitud Seguridad Confidencialidad Calidad de los datos

	relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.	archivos, registros, bancos de datos u otros métodos técnicos de tratamiento de datos, ya sean estos públicos o privados destinados a proporcionar informes, con el fin de asegurar el derecho al honor y a la privacidad de las personas, así como también el acceso a la información que se registre sobre ellas, de acuerdo con lo dispuesto en el tercer párrafo del artículo 43.	

Nota. Elaboración propia.

III Potencial de impacto y posibles reformas a las leyes colombianas

3.1 Resultados

A partir del ejercicio comparativo entre el marco legislativo relacionado a la protección de datos entre Colombia, México, Argentina y la UE, resulta evidente el potencial impacto que tendrían las reformas propuestas a la norma colombiana. Ahora bien, se encontró que este impacto resulta ser significativo y multifacético, debido a que dichas reformas no solo buscan fortalecer el marco legal, sino que también promueven una cultura de privacidad digital en el país.

Por un lado, la reforma al artículo 15 de la Constitución Política de Colombia –que garantiza el derecho a la intimidad personal y familiar y la inviolabilidad de la correspondencia y las comunicaciones privadas– puede tener una repercusión profunda en la protección de la privacidad en la era digital, teniendo en cuenta que este artículo, en su forma

actual, se redactó antes de la explosión de la tecnología digital y de las redes sociales. Por lo tanto, una actualización de este debe reflejar los desafíos modernos en materia de privacidad. En ese sentido, una reforma resulta crucial para proporcionar una base sólida que permita la creación de leyes y políticas capaces de proteger eficazmente los datos personales, atendiendo a las necesidades de esta era en que las amenazas a la privacidad son omnipresentes y sofisticadas. Por lo tanto, actualizar este artículo puede asegurar que la Constitución Política contemple explícitamente las nuevas formas de comunicación y almacenamiento de datos, debido a que de esta forma se brindaría una protección más robusta y específica contra la vulneración de la privacidad.

Por otro lado, la Ley 1581 de 2012, que establece las bases para la protección de los datos personales en Colombia, también requiere reformas, en las que es esencial incluir disposiciones más claras y estrictas sobre la recolección, almacenamiento y el uso de datos personales. Por consiguiente, se determinó que estas reformas deben alinearse con mejores prácticas internacionales, como las establecidas en el GDPR de la UE, elevando así el estándar en Colombia, lo cual puede ofrecer una mayor protección a los ciudadanos y aumentar la confianza en el manejo de sus datos personales, así como establecer directrices precisas sobre cómo las empresas y entidades deben manejarlos.

Como resultado, esto reducirá el riesgo de mal manejo y el abuso de la información. Por ende, aunque la Ley 1266 de 2008 tiene el objetivo de regular el manejo de información crediticia y financiera, es necesario modificarla para extender sus principios a otros tipos de datos personales. Esto incluiría procedimientos de rectificación, control y eliminación de información personal.

Finalmente, la Sentencia T-280 de 2022, enfocada en la importancia de la protección de datos personales, destaca la necesidad de una tutela eficaz contra la difusión no autorizada de información íntima y, en esa medida, propone incluir mecanismos más efectivos para sancionar conductas que violen el derecho a la privacidad, así como también implementar criterios específicos sobre violencia de género en este contexto, con el fin de ofrecer una protección más comprensiva y justa a las víctimas y, sobre todo, promover la educación respecto a la privacidad digital. Esto puede lograrse mediante:

- La implementación de programas educativos que informen a los ciudadanos sobre sus derechos y responsabilidades en el manejo de información personal.
- Campañas de sensibilización que empoderen a los ciudadanos para tomar decisiones informadas y adoptar prácticas seguras en el uso de tecnologías digitales.

Todo lo anterior demuestra que las reformas propuestas al artículo 15 de la Constitución Política de Colombia, junto con la actualización de las leyes 1581 de 2012 y 1266 de 2008, tienen el potencial de mejorar significativamente la protección del derecho a la privacidad en el país. En consecuencia, estas medidas aseguran una respuesta más eficaz ante los desafíos de la era digital, debido a que protegen mejor a los ciudadanos frente a la difusión no autorizada de su información privada.

Asimismo, promover la educación sobre privacidad digital complementa estas reformas, lo que genera conciencia en la población sobre la importancia de la protección de sus datos personales de manera efectiva. En resumen, la actualización y el fortalecimiento de las leyes y políticas de privacidad en Colombia es una necesidad urgente para afrontar los retos de la era digital y asegurar la salvaguarda de los derechos esenciales de las personas.

IV Conclusiones

Esta investigación adoptó un enfoque cualitativo y un diseño exploratorio-descriptivo y otro expositivo-comparativo, con el objetivo de analizar el marco normativo y jurisprudencial de Colombia alrededor de la protección del derecho a la privacidad en un entorno digital. Como resultado, este enfoque permitió una comprensión profunda y detallada de las complejidades y deficiencias del marco legal vigente, así como una comparación con modelos internacionales, particularmente con el GDPR de la UE.

De igual modo, a través de una revisión minuciosa de la legislación y jurisprudencia colombiana, incluyendo el artículo 15 de la Constitución Política, la Ley 1266 de 2008 y la Ley 1581 de 2012, se identificaron debilidades y vacíos en la protección de datos personales. En tal sentido, el análisis comparativo con el GDPR y las legislaciones de México y Argentina reveló la necesidad de alinear las normativas colombianas con las mejores prácticas internacionales para fortalecer la protección de la privacidad. Asimismo, en el estudio se evaluaron casos prácticos de Colombia donde se vulneró este derecho fundamental, lo que posibilitó identificar patrones y desafíos en la implementación de las leyes existentes.

Finalmente, este trabajo destacó la importancia de promover la educación sobre privacidad digital, concienciar a la población sobre la importancia de proteger sus datos personales e incentivar a tomar decisiones informadas para una protección efectiva. En suma, la implementación de programas educativos y campañas de sensibilización se presenta como

una estrategia complementaria esencial para reforzar la cultura de privacidad y seguridad digital en Colombia.

En conclusión, esta investigación subrayó la necesidad urgente de modernizar y fortalecer las leyes y políticas de privacidad en Colombia para abordar los desafíos de la era digital. Por consiguiente, se determinó que las reformas sugeridas, alineadas con estándares internacionales, junto con una robusta educación sobre privacidad digital, son esenciales para garantizar la protección de los derechos fundamentales de los ciudadanos en un entorno cada vez más digitalizado.

V. Referencias

Aguado, E. S. (2014). El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones. *Revista del Instituto Español de Estudios Estratégicos*, (4). https://revista.ieee.es/article/view/306/507

Ámbito Jurídico. (3 de julio de 2013). *SIC confirma sanción a Bel Star por violar las normas sobre hábeas data crediticio (8:30 a.m.).* Ámbito jurídico https://www.ambitojuridico.com/noticias/mercantil/financiero-cambiario-y-seguros/sic-confirma-sancion-bel-star-por-violar-las

Arévalo, Y. (2020). *Protección de datos personales en Colombia frente al profiling y entornos digitales* [Tesis de grado]. Universidad Santo Tomás. (CRAI-USTA) http://hdl.handle.net/11634/31170

Ayala, J., Ariza, J., & González, L. (2020). La protección de datos en la era digital Colombia - España. *Revista Politécnico Grancolombiano*. http://hdl.handle.net/10823/2142

Baquero, H. A. (2015). *Ley 1581 de 2012 protección de datos personales en Colombia*. Universidad Piloto de Colombia. https://repository.unipiloto.edu.co/handle/20.500.12277/8576

Berro, G. (2013). Consentimiento informado. *Revista Uruguaya de Cardiología, 28*(1), 17-31. https://www.redalyc.org/articulo.oa?id=479748558007

Carreño, B., & Baquero, W. (2023). *Política criminal del delito informático en Colombia.* [Tesis de grado, Universidad Santo Tomás]. (CRAI-USTA). http://hdl.handle.net/11634/50772

Congreso de la República de Colombia. Ley 1581/12 [Ley de Protección de Datos Personales],17 de octubre de 2012.

Congreso de la República de Colombia. Ley 1266/08 [Ley de Habeas Data], 31 de diciembre de 2008.

Congreso General de los Estados Unidos Mexicanos. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 26 de enero de 2017-

Consejo Federal para la Transparencia. (2022). *Informe sobre la actualización de la Ley de Protección de Datos Personales desde una perspectiva federal*. Agencia de Acceso a la Información Pública. https://www.argentina.gob.ar/aaip/consejo-federal-transparencia

Constitución Política de Colombia [C.P.]. (1991). Legis.

Corte Constitucional, Sala Octava de Revisión de tutelas. Sentencia T280/22 [M. P: Reyes, C.], 8 de agosto de 2022.

Corte Constitucional, Sala Segunda de Revisión de tutelas. Sentencia T-339/22, [M.P: Ibáñez, N.,28 de septiembre de 2022.

Departamento de Derecho Internacional. (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.* Comité Jurídico Interamericano, Organización de los Estados Americanos [OEA]. https://www.oas.org/es/sla/cji/informes_culminados_recientemente_Proteccion_Datos_Personales.asp

Forero, D., & Vélez, S. (2016). *Ley 1581 de 2012: Contextualización de la norma a nivel nacional e internacional y análisis de algunas sanciones interpuestas* [Tesis de grado]. Universidad Pontificia Bolivariana. http://hdl.handle.net/20.500.11912/2886

Franco, Z. R. (2005). El consentimiento informado como ejercicio de la autonomía en promoción de la salud. *Hacia La Promoción de La Salud, 10,* 48–58. https://revistasojs.ucaldas.edu.co/index.php/hacialapromociondelasalud/article/view/1922

Galvis, L. (2012). Protección de datos en Colombia, avances y retos. *Revista Lebret, 4*(4), 195-214. https://doi.org/https://doi.org/10.15332/rl.v4i4.336

Gregorio, C. (2005). Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina. En Concha, H; López-Ayllón, S & Tacher Epelstein, L. (Coord.), *Transparentar al estado: la experiencia mexicana de acceso a la información.* RU Jurídicas.

Mancera, A. (2013). *Confirman sanción a Bel Star por violar Hábeas Data*. Asuntos legales. https://www.asuntoslegales.com.co/actualidad/confirman-sancion-a-bel-star-por-violar-habeas-data-2041886

Montero, E. (2008). *El funcionalismo penal. Una introducción a la teoría de Günther Jakobs*. Revista electrónica Derecho Penal Online. https://derechopenalonline.com/el-funcionalismo-penal-una-introduccion-a-la-teoria-de-gunther-jakobs/

Moreno, I. J. & Olmeda, M. D. P. (2022). Derecho a la privacidad en la sociedad de la información. *Advocatus, 19* (37), 15-27. https://doi.org/10.18041/0124-0102/a.37.8161

Nader, R. (2020). Ley orgánica de regiones: antecedentes y principales aspectos de la Ley 1962 de 2019. *Advocatus*, *18* (35), 15-38. https://doi.org/10.18041/0124-0102/a.35.6896

Orejarena, A. (2021). *Vulneración del derecho a la intimidad de niños, niñas y adolescentes a causa de la publicación indiscriminada de sus fotografías en plataformas digitales "sharenting en el contexto colombiano"* [Tesis de grado]. Universidad Santo Tomás. http://hdl.handle.net/11634/35120

Peña, Y. A. (2018). *Retos regulatorios de la protección de datos en Colombia* [Tesis de maestría]. Universidad Santo Tomás. https://repository.usta.edu.co/handle/11634/14709

Pfeiffer, M. L. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética, 3*(1), 11-36. https://www.redalyc.org/articulo.oa?id=189217248002

Piñar, J.L. (Dir.). (2016). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. Editorial Reus.

Quiñones, D. M. (Comp.). (2022). *10 años de la ley de Protección de datos: ¿Qué tanto hemos avanzado? ¿qué nos hace falta? La ley al tablero*. Universidad Externado de

Colombia. https://www.uexternado.edu.co/evento/departamento-de-derecho-comunicaciones-y-tecnologias-de-la-informacion/10-anos-de-la-ley-de-proteccion-de-datos-que-tanto-hemos-avanzado-que-nos-hace-falta-la-ley-al-tablero/

Riesco, J. (2022). *La libertad de expresión y la privacidad en la era digital* [Tesis de pregrado]. Universidad de Valladolid. https://uvadoc.uva.es/handle/10324/59605

Salamanca, E. (2018). El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones *Revista Del Instituto Español De Estudios Estratégicos*, (4). https://revista.ieee.es/article/view/306

Revista Semana. (2 de julio de 2013). *A Bel Star le faltó comunicación con sus deudores.* https://www.semana.com/empresas/articulo/bel-star-falto-comunicacion-deudores/178948/

Serra, R. (2015). La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional. *Revista de Derecho Político* (92), 73–118. https://doi.org/10.5944/rdp.92.2015.14422

Unidad de Planeación Minero-Energética [UPME]. (2021). *Política de Tratamiento de Datos Personales.* https://www1.upme.gov.co/ServicioCiudadano/Paginas/tratamiento-datos-personales.aspx

Valencia, A. (2016). *El derecho fundamental a la intimidad en el contexto digital de Colombia* [Disertación doctoral]. Universidad Santo Tomás. (CRAI-USTA). https://repository.usta.edu.co/handle/11634/1978