



GERMÁN ROZO
REPRESENTANTE A LA CÁMARA

Bogotá, D.C., 22 de julio de 2026

Señor:

MIGUEL ÁNGEL SÁNCHEZ

SECRETARIO GENERAL

Honorable Cámara de Representantes

Ciudad

REF: RADICACIÓN PROYECTO DE LEY

En mi condición de miembro del Congreso de la República y en uso del derecho consagrado en el artículo 150 de la Constitución Política de Colombia, por su digno conducto me permito poner a consideración de la Honorable Cámara de Representantes el proyecto de ***Ley “Por medio del cual se regulan las plataformas de redes sociales en Colombia y se dictan otras disposiciones generales”***

Del Honorable Congresista,

GERMÁN ROGELIO ROZO ANÍS

Representante a la Cámara

Departamento de Arauca

PROYECTO DE LEY No. _____ de 2026

“Por medio del cual se regulan las plataformas de redes sociales en Colombia y se dictan otras disposiciones generales”

El Congreso de Colombia,

DECRETA

ARTÍCULO 1°. OBJETO. La presente Ley tiene por objeto establecer regulaciones para el uso de las plataformas de redes sociales en Colombia, con el fin de garantizar la seguridad digital de los ciudadanos, proteger a los menores de edad y establecer mecanismos de responsabilidad para las plataformas que operan en el país. Se busca equilibrar la libertad de expresión con la protección de los derechos fundamentales de los usuarios.

ARTÍCULO 2°. ÁMBITO DE APLICACIÓN. La presente Ley aplica a todas las plataformas de redes sociales que operan en Colombia, ya sean nacionales o extranjeras, y a todos los usuarios dentro del territorio nacional. Asimismo, establece obligaciones para las entidades gubernamentales encargadas de la regulación y supervisión del uso de redes sociales.

ARTÍCULO 3°. DEFINICIONES: Para efectos de la presente Ley se adoptarán las siguientes definiciones:

1. Redes Sociales: Son las interacciones dadas en plataformas digitales formadas por comunidades de individuos con intereses, actividades o relaciones en común. Las redes sociales permiten el contacto entre personas y funcionan como un medio para comunicarse e intercambiar información y/o contenidos.

2. Plataforma de Redes Sociales: Servicio o aplicación basado en Internet que tiene usuarios y cumple con cualquiera de los dos criterios siguientes:

1. El servicio o la aplicación permite a los usuarios interactuar socialmente entre sí dentro del servicio o la aplicación; y

2. El servicio o la aplicación permite a un usuario:

(A) Convertirse en un usuario registrado, establecer una cuenta o construir un perfil público o semipúblico con el fin de iniciar sesión y usar el servicio o la aplicación; y

(B) Crear o publicar contenido que sea visible para otros usuarios.

(C) Ofrecer contenidos de forma gratuita o a cambio de pago hacia usuarios.

3. Cuenta de Redes Sociales: Se define como un perfil en línea creado en plataformas como Facebook o X, que representa a una persona o empresa. Puede usarse para comunicarse, compartir información e interactuar con otros.

4. Usuario: Individuo que crea una cuenta de perfil en una aplicación o sitio web con el objetivo de participar en las dinámicas propias de la plataforma digital.

5. Verificación de Identidad: Procedimiento por el cual una plataforma confirma la identidad de sus usuarios mediante mecanismos de autenticación seguros.

ARTÍCULO 4º. PRINCIPIOS. La presente Ley se regirá por los siguientes principios:

- 1. Seguridad Digital:** Garantizar la protección de los usuarios ante amenazas cibernéticas y fraudes.
- 2. Protección de los menores:** Implementación de medidas estrictas para evitar el acceso de menores de 14 años a plataformas de redes sociales y/o cuentas de redes sociales.
- 3. Responsabilidad de las Plataformas:** Obligación de las empresas de redes sociales de garantizar el cumplimiento de las disposiciones establecidas en esta Ley.
- 4. Libertad de Expresión:** Respeto al derecho de expresión de los usuarios, sin menoscabo de los límites establecidos en la legislación nacional e internacional.

ARTÍCULO 5º. OBLIGACIÓN DE VERIFICACIÓN DE IDENTIDAD. Las plataformas de redes sociales que operen en Colombia deberán implementar un mecanismo obligatorio de verificación de identidad para todos los usuarios utilizando tecnologías seguras que garanticen la autenticidad de la información proporcionada por los mismos.

ARTÍCULO 6º. RESTRICCIÓN DE ACCESO A MENORES DE 14 AÑOS. Las plataformas de redes sociales tendrán la obligación de restringir el acceso y el registro de menores de 14 años, salvo en aquellas diseñadas específicamente para menores con control parental y aprobación expresa de sus representantes legales.

ARTÍCULO 7º. DERECHOS DE LOS USUARIOS. Todo usuario tendrá derecho a:

1. Recibir notificación motivada ante sanciones o bloqueos.
2. Apelar decisiones de moderación ante la plataforma.
3. Acceder a reportes de transparencia sobre el uso de algoritmos, publicidad dirigida y moderación de contenido.

ARTÍCULO 8º. MECANISMOS DE DENUNCIA. Las plataformas deberán implementar mecanismos de denuncias rápidos y eficientes para que los usuarios puedan reportar contenido ilegal o que vulnere derechos fundamentales, garantizando una respuesta oportuna y eficaz a las solicitudes.

ARTÍCULO 9º. TRANSPARENCIA EN LOS TÉRMINOS Y CONDICIONES. Las plataformas deberán garantizar que sus términos y condiciones sean claros, accesibles y cumplan con la legislación colombiana, incluyendo la especificación de los mecanismos de verificación de identidad y protección de menores.

PARÁGRAFO 1. Las plataformas de redes sociales tendrán la obligación de:

1. Publicar informes semestrales sobre contenido eliminado, causas, tiempos de respuesta, y recursos interpuestos.
2. Informar de forma clara el funcionamiento de sus algoritmos de recomendación, publicidad y eliminación de contenido.
3. Notificar a los usuarios sobre cualquier uso de sus datos y obtener consentimiento informado.

ARTÍCULO 10°. PROHIBICIONES. Para efectos de la presente Ley, queda prohibida:

1. La creación de cuentas falsas o el uso de identidades ficticias en redes sociales.
2. El registro y acceso de menores de 14 años a plataformas no diseñadas específicamente para su uso.
3. La difusión de información falsa con la intención de manipular la opinión pública o difamar a personas naturales o jurídicas.
4. La retención de datos personales de usuarios sin su expreso consentimiento.

ARTÍCULO 11°. PROCEDIMIENTO Y SANCIONES ADMINISTRATIVAS. Las plataformas de redes sociales que incumplan las disposiciones de esta Ley serán objeto de sanciones y multas.

El proceso administrativo sancionatorio aquí dispuesto, estará a cargo de la Superintendencia de Industria y Comercio - SIC-, o quienes hagan sus veces; y observarán las reglas establecidas en el Capítulo III del Título III de la Parte Primera de la Ley 1437 de 2011 (CPACA), o por las normas que la modifiquen, adicionen o sustituyan.

La plataforma digital de red social que incumpla lo dispuesto en esta Ley, incurrirá en multa de hasta cinco mil (5.000) salarios mínimos legales mensuales vigentes y la autoridad sancionadora podrá dictaminar el Bloqueo temporal o permanente de la operación en Colombia en casos de incumplimientos reiterados.

PARÁGRAFO: Los criterios de graduación de las sanciones y multas que observarán la Superintendencia de Industria Comercio, serán los establecidos en el Parágrafo 1° del Artículo 61 de la Ley 1480 de 2011 -Estatuto del Consumidor y deberán tener en cuenta el principio de proporcionalidad de las sanciones.

ARTÍCULO 12°. AUTORIDAD REGULADORA. La Superintendencia de Industria y Comercio será la entidad encargada de supervisar el cumplimiento de esta Ley y de imponer sanciones a las plataformas que infrinjan las disposiciones establecidas.

ARTÍCULO 13°. OFICINA FÍSICA EN COLOMBIA. Toda plataforma de redes sociales o empresa que preste estos servicios en Colombia y supere los 100.000 usuarios activos deberá contar con una oficina física en el país. Esta oficina deberá servir como canal de atención a autoridades regulatorias, usuarios y procesos judiciales, y

garantizar una representación legal con capacidad de respuesta frente a las obligaciones establecidas en esta Ley.

ARTÍCULO 14°. REGLAMENTACIÓN Y PERIODO DE TRANSICIÓN. El Gobierno Nacional reglamentará lo dispuesto en la presente Ley en un término de doce (12) meses contados a partir de su entrada en vigencia.

PARÁGRAFO: Las plataformas de redes sociales sujetas a la presente Ley contarán con un período de transición de hasta doce (12) meses contados a partir de la entrada en vigencia de la Ley para adecuar sus políticas, sistemas y operaciones a las disposiciones aquí establecidas. Vencido el período de transición, toda plataforma que no haya cumplido con las obligaciones definidas en la presente ley podrá ser objeto de sanciones conforme a lo establecido en el artículo

ARTÍCULO 15°. VIGENCIA. La presente ley entrará a regir a partir de su promulgación y publicación y deroga las disposiciones que le sean contrarias.

Del Honorable Congresista,

GERMAN ROGELIO ROZO ANIS

Representante a la Cámara
Departamento de Arauca

EXPOSICIÓN DE MOTIVOS

1. ANTECEDENTES LEGISLATIVOS

El presente proyecto de Ley fue previamente radicado en la Cámara de Representantes el 22 de julio de 2025, bajo el número 074 de 2025 Cámara, siendo de iniciativa parlamentaria suscrito por los congresistas H.R Germán Rogelio Rozo Anís y H.R. Hugo Alfonso Archila Suárez.

Fue radicada la ponencia para primer en la Comisión Sexta de la Cámara de Representantes, sin embargo, no fue debatido un aprobado por lo que fue archivado en consideración a lo dispuesto en el artículo 190 de la Ley 5 de 1992. No obstante, lo anterior, atendiendo a la importancia que reviste para la actualidad del país y para la protección de los menores de edad, se vuelve a presentar ante el Congreso de la República.

Finalmente, en el texto propuesto se recogen las recomendaciones técnicas realizadas por la Comisión de Regulación de Comunicaciones mediante concepto, y que se reflejan dentro de la presente iniciativa.

2. JUSTIFICACIÓN DE LA INICIATIVA

En la era digital, las redes sociales se han convertido en un espacio fundamental para la comunicación, la información y la interacción entre personas, empresas e instituciones. En Colombia, el uso de estas plataformas ha crecido exponencialmente, convirtiéndose en una herramienta indispensable para la vida cotidiana de millones de ciudadanos. Según el estudio We Are Social de Meltwater, en febrero de 2024 se registraron 36,80 millones de usuarios activos en redes sociales en el país, evidenciando su masiva adopción y el impacto que generan en la sociedad.¹ Este crecimiento plantea retos significativos en términos de regulación, seguridad digital y protección de derechos fundamentales.

Si bien estas plataformas han facilitado la conexión y el acceso a información, también han planteado retos significativos en materia de seguridad digital, protección de menores, desinformación y privacidad de los datos. El auge de problemáticas como la suplantación de identidad, la difusión de contenido nocivo y la manipulación de información requiere una regulación clara y efectiva que garantice el equilibrio entre la libertad de expresión y la protección de los derechos fundamentales de los ciudadanos.

Las redes sociales han permitido que la información viaje con una rapidez sin precedentes, permitiendo a los ciudadanos estar informados en tiempo real sobre eventos nacionales e internacionales. Sin embargo, esta inmediatez también ha

¹<https://www.portafolio.co/tecnologia/estas-son-las-redes-sociales-mas-usadas-por-loscolombianos-616960>

facilitado la propagación de noticias falsas y contenido malintencionado, lo que puede generar desinformación, confusión y pérdida de confianza en las instituciones. En Colombia, el impacto de la desinformación ha sido un factor relevante en distintos procesos democráticos y en la estabilidad social, lo que hace imperativa la adopción de medidas regulatorias que establezcan mecanismos eficaces para combatir estos fenómenos sin menoscabar la libertad de expresión.

En este contexto, el presente Proyecto de Ley busca establecer un marco normativo que regule el funcionamiento de las plataformas de redes sociales en Colombia. Con el objetivo de promover un entorno digital seguro y responsable, esta iniciativa legislativa establece lineamientos para la verificación de identidad de los usuarios, la protección de menores de edad, la transparencia en los términos y condiciones de uso y la creación de mecanismos eficaces de denuncia ante vulneraciones de derechos. Esta regulación no solo beneficiará a los usuarios, sino que también proporcionará un marco legal claro para las plataformas digitales, garantizando su operación en condiciones justas y seguras.

El impacto de las redes sociales en la sociedad es innegable. En plataformas como Facebook, Instagram, YouTube y TikTok, millones de colombianos interactúan diariamente, accediendo a contenidos que influyen en su percepción del mundo y en sus decisiones personales y profesionales. La regulación propuesta en este Proyecto de Ley no busca restringir el acceso a estas herramientas, sino establecer normas que favorezcan un uso responsable y seguro, alineado con las mejores prácticas internacionales y con el respeto a los derechos fundamentales.

Uno de los aspectos más críticos que aborda esta ley es la protección de los menores de edad. La presencia de niños y adolescentes en redes sociales los expone a numerosos riesgos, incluyendo el acoso, el ciberbullying, la explotación infantil y el acceso a contenidos inadecuados. En Colombia, la falta de un marco regulatorio ha permitido que menores de edad accedan sin restricciones a estas plataformas, sin mecanismos efectivos de supervisión por parte de las empresas tecnológicas. La presente iniciativa legislativa establece la obligatoriedad de medidas estrictas para restringir el acceso de menores de 14 años a plataformas no diseñadas específicamente para su uso, asegurando un entorno digital más seguro para las futuras generaciones.

Además de la protección de menores, esta ley enfatiza la necesidad de establecer mecanismos de verificación de identidad para combatir la creación de cuentas falsas y la suplantación de identidad. La falta de verificación en redes sociales ha facilitado la proliferación de perfiles anónimos utilizados para cometer delitos como estafas, extorsión y acoso. La implementación de mecanismos seguros de verificación de identidad contribuirá a reducir estos delitos y fortalecerá la seguridad digital en el país.

Otro punto relevante de esta iniciativa es la regulación de la retención y uso de datos personales por parte de las plataformas. En la actualidad, muchas empresas tecnológicas almacenan y procesan información de los usuarios sin su

consentimiento explícito, lo que plantea serios riesgos en términos de privacidad y protección de datos. Esta ley busca garantizar que el tratamiento de datos personales cumpla con los principios de transparencia, legalidad y consentimiento informado, asegurando que los usuarios tengan pleno control sobre su información.

En síntesis, este proyecto responde a la necesidad de un marco regulador que brinde garantías tanto a los usuarios como a las plataformas, promoviendo un ecosistema digital más seguro y confiable. La protección de la información personal, la prevención de riesgos para menores de edad y la responsabilidad de las plataformas en la gestión de contenidos son aspectos esenciales que esta legislación pretende abordar, en consonancia con el desarrollo tecnológico y la evolución de la sociedad digital en Colombia. Al establecer reglas claras y mecanismos de cumplimiento, esta ley contribuirá a fortalecer la confianza en el entorno digital y a garantizar que las redes sociales continúen siendo espacios de interacción seguros y responsables para todos los colombianos.

1.1 Uso de las redes sociales en Colombia

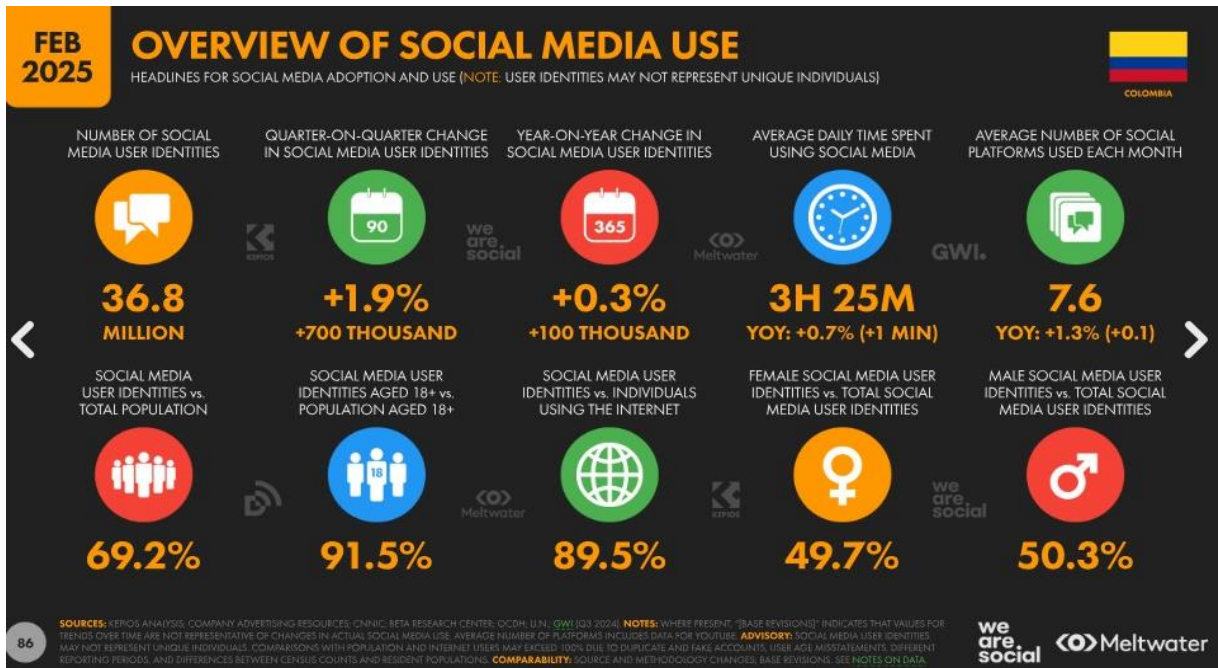
En enero de 2025, Colombia registró 36.8 millones de usuarios activos en redes sociales, equivalente al 69.2 % de la población total. Este crecimiento ha convertido a las plataformas digitales en un eje central de la comunicación y la interacción social en el país. Sin embargo, el incremento en su uso también ha generado desafíos en materia de seguridad digital, protección de datos y control de contenido.

El análisis de la fundación Melwater a 2025 muestra que el 91.5 % de los colombianos mayores de 18 años utilizan redes sociales, con una distribución de género equilibrada (49.7 % mujeres y 50.3 % hombres). Además, el país es el sexto a nivel mundial en tiempo de uso diario de estas plataformas, con un promedio de 3:25 horas al día, muy por encima del promedio global de 2:21 horas. Esta tendencia evidencia la creciente dependencia de la población colombiana en las redes sociales no solo para el entretenimiento, sino también para el acceso a información, la interacción social y la realización de actividades laborales y comerciales.²

Las redes sociales más utilizadas en Colombia incluyen Facebook, TikTok, Instagram, YouTube, LinkedIn, Pinterest, X (Twitter) y Snapchat. Estas plataformas tienen un impacto significativo en el acceso a la información, la interacción social y la actividad comercial. Facebook sigue siendo la red con mayor alcance, con 36.8 millones de usuarios (69.2 % de la población), seguida de TikTok con 32 millones y YouTube con 30.6 millones. Instagram, con 20.4 millones de usuarios, se mantiene como una plataforma clave, especialmente entre jóvenes y adultos jóvenes.

Gráfico 1. Resumen del uso de redes sociales en Colombia a febrero de 2025

² We Are Social & Meltwater. (2025). *Digital 2025 Global Overview Report: The Essential Guide to the World's Connected Behaviours*. We Are Social.

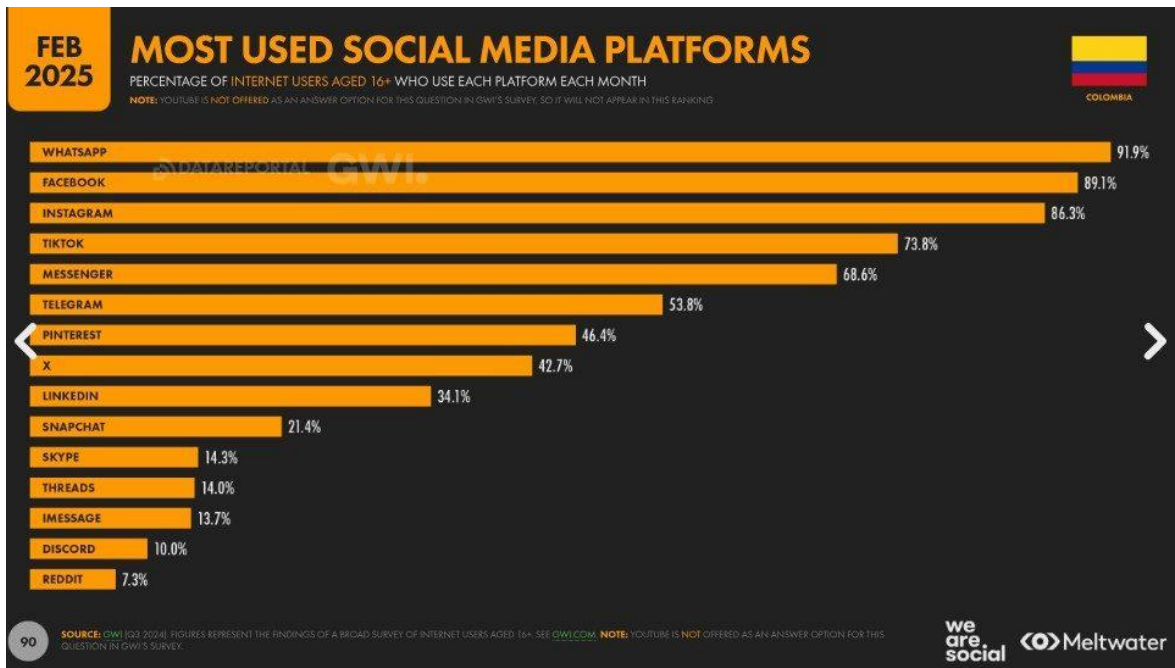


Fuente: Digital 2025 Global Overview Report: The Essential Guide to the World's Connected Behaviour

El crecimiento de plataformas como TikTok (+17.1 % en un año) y LinkedIn (+23.1 %) refleja la diversificación de las preferencias digitales de los colombianos. Sin embargo, también se ha evidenciado una disminución en plataformas como X (Twitter), que perdió 410 mil usuarios en el último año. Estos cambios en la dinámica de uso reflejan la necesidad de establecer una regulación flexible que se adapte a la evolución del ecosistema digital.

El acceso masivo a estas plataformas implica una serie de riesgos, incluyendo la propagación de desinformación, la vulnerabilidad de los menores de edad, la suplantación de identidad y el uso indebido de datos personales. En plataformas como TikTok y YouTube, donde el consumo de contenido es mayormente audiovisual y dirigido a públicos jóvenes, la exposición a material inapropiado sin supervisión es una preocupación creciente. Por su parte, en redes como Facebook e Instagram, el alcance de campañas de desinformación ha mostrado una capacidad de influir en la opinión pública, afectando procesos democráticos y decisiones sociales.

Gráfico 2. Redes Sociales más usadas en Colombia

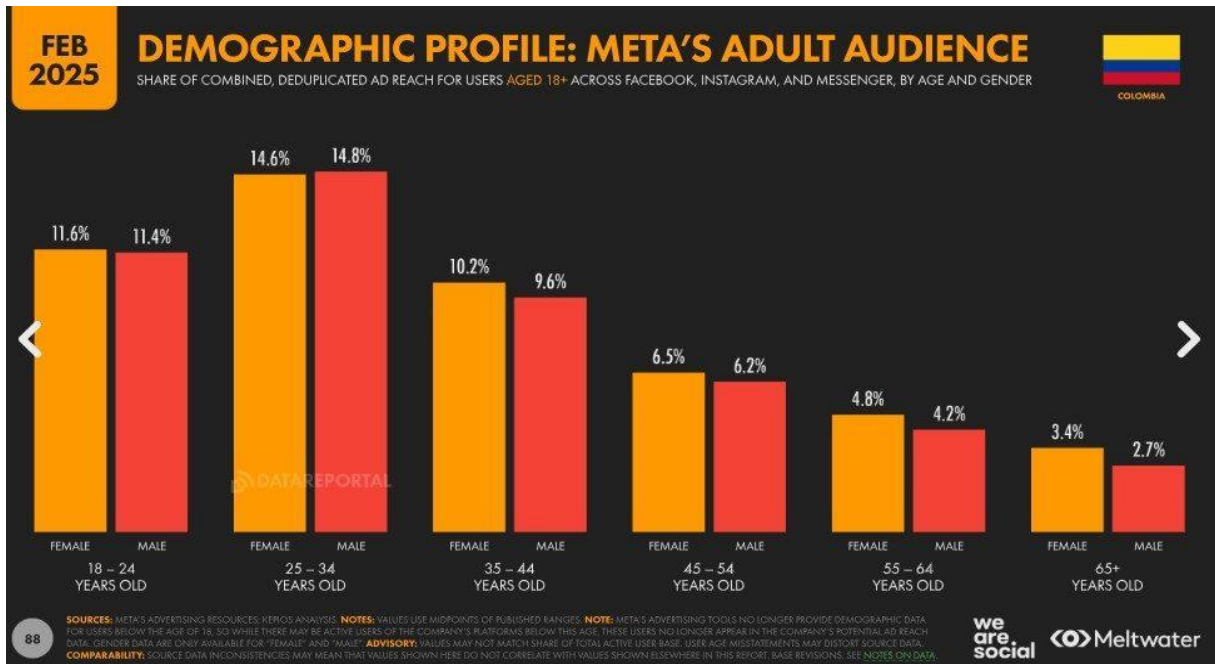


Fuente: Digital 2025 Global Overview Report: The Essential Guide to the World's Connected Behaviour

Otro punto crítico es la comercialización de datos personales y el uso de información de los usuarios con fines publicitarios sin su consentimiento explícito. El crecimiento del mercado digital ha llevado a que estas plataformas acumulen grandes volúmenes de datos de los colombianos, lo que exige una regulación más estricta sobre la privacidad y la seguridad de la información personal.

El fenómeno de las cuentas falsas y la suplantación de identidad es otro problema relevante en el ecosistema digital colombiano. La facilidad para crear perfiles falsos en redes sociales ha generado un aumento en delitos como estafas, acoso y fraude, afectando la seguridad de los usuarios. Las plataformas digitales deben asumir mayores responsabilidades en la verificación de identidad y en la implementación de mecanismos efectivos para detectar y eliminar cuentas fraudulentas.

Gráfico 3. Distribución por género y edad de las redes sociales de Meta (Facebook, Instagram y Mesenger)



Fuente: Digital 2025 Global Overview Report: The Essential Guide to the World's Connected Behaviour

El presente Proyecto de Ley responde a la necesidad de regular de manera efectiva el ecosistema digital en Colombia, garantizando la seguridad y transparencia en el uso de redes sociales, protegiendo a los menores de edad y estableciendo mecanismos de responsabilidad para las plataformas tecnológicas que operan en el país. La legislación propuesta busca equilibrar la libertad de expresión con la protección de los derechos fundamentales, asegurando que la innovación tecnológica se desarrolle dentro de un marco que priorice el bienestar de los ciudadanos.

En este sentido, se propone establecer obligaciones claras para las plataformas en cuanto a la gestión de contenido sensible, la verificación de identidad de usuarios y la implementación de herramientas efectivas para la denuncia y eliminación de contenido ilegal. Además, se busca fomentar la alfabetización digital para que los colombianos puedan hacer un uso más informado y seguro de estas plataformas. Dado el impacto de las redes sociales en la vida cotidiana de millones de colombianos y el potencial que tienen para influir en la sociedad, la regulación en este ámbito es un paso fundamental para garantizar un entorno digital más seguro, equitativo y responsable.

1.2 El desafío de la regulación internacional:

Las redes sociales han revolucionado la forma en que los ciudadanos acceden a la información, participan en la vida democrática y se relacionan con su entorno. No obstante, también han introducido desafíos significativos en cuanto a la seguridad digital, la protección de menores y la gobernanza del espacio público en el entorno

digital. En este contexto, la regulación de estas plataformas se ha convertido en una necesidad urgente para garantizar que su uso contribuya al bienestar social sin afectar derechos fundamentales.

A nivel global, se ha evidenciado que las redes sociales pueden ser tanto una herramienta de fortalecimiento de la democracia como un mecanismo de desinformación y manipulación política. Como destaca Nanjala Nyabola en su artículo *Seeing the forest – and the trees: The global challenge of regulating social media for democracy*, "las plataformas digitales han sido clave en la amplificación de movimientos ciudadanos como *Black Lives Matter* o *Rhodes Must Fall*, pero también han sido utilizadas por actores malintencionados para socavar la democracia mediante redes de desinformación y manipulación algorítmica". Esto muestra que, aunque las redes sociales pueden ser un motor de cambio positivo, también pueden convertirse en herramientas de influencia negativa si no se regulan adecuadamente.

Además, Nyabola resalta que "el potencial de socavar la democracia es a veces una consecuencia de las características incorporadas en las redes sociales, como la tendencia a reforzar perspectivas insulares y la posibilidad de comprar influencia o visibilidad en estas plataformas".³ Este es un punto crítico en el debate sobre la regulación, ya que muchas redes sociales operan con modelos de negocio que priorizan el engagement sobre la veracidad de la información, lo que puede exacerbar la polarización y el impacto negativo en la democracia.

El crecimiento de las redes sociales ha convertido a estas plataformas en negocios transnacionales con un poder significativo sobre la información y la privacidad de los usuarios. Como señala Nyabola, "Meta y Alphabet han acumulado cantidades masivas de datos, lo que ha generado preocupaciones sobre el uso y la monetización de la información personal sin el debido consentimiento de los usuarios". Esta acumulación de datos ha llevado a que muchas plataformas "no solo actúen como redes sociales, sino como grandes empresas de recolección de información personal para la monetización en publicidad y análisis de comportamiento".

1.3 Transparencia en la información:

Una de las principales preocupaciones del público en relación con la regulación de las redes sociales es la **transparencia**. Las investigaciones que examinan la opinión pública y de los usuarios sobre la moderación de contenido han identificado esta cuestión tanto desde la perspectiva de los usuarios como desde la eficacia regulatoria. Esto se refleja en muchas de las prácticas de moderación y censura aplicadas por las plataformas de redes sociales, aunque a menudo se identifica como un problema tanto para la moderación realizada por humanos como para la basada en algoritmos. La opinión de los usuarios tiende a depositar mayor

³ Nanjala Nyabola (2023) *Seeing the forest – and the trees: The global challenge of regulating social media for democracy*, South African Journal of International Affairs, 30:3, 455-471

confianza en las prácticas de moderación que muestran más transparencia, aunque esto sea en ocasiones difícil de alcanzar para las plataformas sociales.⁴

La falta de transparencia da lugar a la aparición de teorías entre los usuarios, quienes, al intentar comprender prácticas de moderación que pueden parecer secretas o mal explicadas, desarrollan sus propias hipótesis sobre por qué se eliminó cierto contenido. Myers West (2018) encontró que la teoría más común elaborada por los usuarios era que alguien había reportado su contenido, y que se trataba de otro usuario regular, y no de un moderador encargado de identificar contenido problemático. Algunos usuarios incluso afirmaban que alguien con una postura contraria a sus publicaciones había actuado en su contra, o que un moderador humano específico representaba las posiciones políticas e ideológicas de la empresa de redes sociales.⁵

Las leyes y los enfoques regulatorios impulsados por las plataformas son más eficaces cuando cuentan con la aceptación de los usuarios y con su confianza en el proceso de moderación.⁶ Esto es especialmente relevante cuando se suspenden cuentas o se eliminan grandes cantidades de contenido con base en decisiones que se comunican sin detalles específicos.

La falta de transparencia genera sospechas entre los usuarios, quienes pueden asumir que la plataforma y los procesos de moderación tienen algún tipo de sesgo en su contra.⁷ Una mayor transparencia y el intercambio de información sobre los procesos y decisiones de moderación no solo incrementan la satisfacción de los usuarios, sino que también les ayuda a comprender cómo deben comportarse en línea. Existe el riesgo de que las regulaciones basadas en tecnología —como el análisis de contenido en redes sociales mediante inteligencia artificial— se perciban como inherentemente opacas por parte de los usuarios. En consecuencia, la legitimidad de este tipo de regulación puede ser cuestionada por quienes no tienen acceso, conocimiento ni control sobre cómo se diseña y aplica dicho proceso

Así, el público percibe las redes sociales como plataformas públicas que “desempeñan un papel cívico cada vez más importante como espacios para el debate”, y como un lugar colectivo donde los usuarios pueden compartir e

⁴ Christine Cook, Aashka Patel, and Donghee Wohn, ‘Commercial Versus Volunteer: Comparing User Perceptions of Toxicity and Transparency in Content Moderation Across Social Media Platforms’ (2021) *Frontiers in Human Dynamics* <www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2021.626409/full> accedido marzo de 2025.

⁵ Sarah Myers West, ‘Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms. [2018] *New Media & Society* 4366.

⁶ Nicolas Suzor et al, ‘What Do We Mean When We Talk About Transparency? Towards Meaningful Transparency in Commercial Content Moderation’ [2019] 13 *International Journal of Communication* 1526.

⁷ Shagun Jhaver, Amy Bruckman, and Eric Gilbert, ‘Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit’ [2019] 3 *Proceedings of the ACM on Human-Computer Interaction* 1.

intercambiar ideas e información⁸. Esta percepción ha sido promovida por las propias plataformas, ya que está alineada con sus intereses. La legitimidad percibida que esto genera involucra tanto a los usuarios como al público en general.

Esto se convierte en un aspecto central al considerar cualquier marco legal o político que busque regular el contenido en redes sociales, especialmente aquel que pueda afectar la seguridad en línea, como el contenido que no se clasifica claramente como “extremista”, pero que podría ser parte de una ideología más amplia.

La cantidad y variedad de contenido que se regula es inmensa y sigue creciendo. En el caso del extremismo, por ejemplo, los reguladores deben moderar y censurar una gama cada vez más diversa de personas y grupos. Muchos de ellos no encajan en la definición formal de “extremista” o “terrorista”, sino que se ubican en los márgenes de posturas políticas más convencionales. Con el auge de nuevos movimientos de extrema derecha, la línea entre la política extremista y la política tradicional se ha vuelto cada vez más difusa.⁹

En este contexto, la presión sobre las plataformas de redes sociales y los organismos reguladores del Estado para que moderen el contenido de una forma que responda tanto a las necesidades de la sociedad como a las expectativas de los usuarios es un desafío complejo, cambiante y altamente politizado.

Los estudios recientes sobre el papel —y quizás más importante aún, la responsabilidad— de los proveedores de redes sociales en la regulación de contenidos han generado varios interrogantes sobre la relación entre el Estado y las empresas. El público, en su doble rol de usuario y creador de contenido, constituye un tercer actor clave.¹⁰ Al analizar cómo se regula el contenido problemático que afecta la seguridad en línea —como el contenido extremista—, la interacción entre estos tres actores se vuelve especialmente relevante.¹¹

En este “ensamblaje”, el Estado busca promover la seguridad de sus ciudadanos, y las plataformas de redes sociales se han convertido en una parte fundamental de esa estrategia. Esto puede interpretarse como una extensión de las prácticas regulatorias del gobierno, que cada vez más complementa las medidas legales con estrategias “más suaves” que incentivan la colaboración de actores privados.

Las investigaciones han demostrado que cuando los usuarios —incluso aquellos que han sido censurados o expulsados— perciben las intervenciones como justas desde el punto de vista procedimental, es menos probable que repitan el

⁸ Myers West (n 15).

⁹ Alastair Reed and Adam Henschke, ‘Who Should Regulate Extremist Content Online?’ in *Counter Terrorism Ethics and Technology* (Springer 2021) 175–98.

¹⁰ Margurite Borelli, ‘Social Media Corporations as Actors of Counter-Terrorism’ [2021] 25 *New Media and Society* 2877.

¹¹ *Ibid*

comportamiento en el futuro. Como señalaron Riedl y otros (2021), la autorregulación también depende de la percepción del usuario sobre la legitimidad de las medidas. Por ejemplo, cuando la libertad de expresión es un valor político central, los usuarios pueden considerar la regulación como ilegítima y mostrarse menos dispuestos a autorregularse.

Además, si los usuarios no respaldan los enfoques regulatorios, no solo es más probable que incurran en conductas negativas, sino que también pueden intentar activamente sabotear las prácticas de regulación de las plataformas. Las redes sociales son, en definitiva, entidades corporativas con un gran poder, el cual pueden ejercer para influir en los procesos regulatorios, y ese es un problema de fondo que no puede pasarse por alto.¹²

Existe un límite a la intervención del Estado establecido por la ley, el cual determina hasta dónde puede censurar a los ciudadanos, y este límite varía según la jurisdicción. Al mismo tiempo, las empresas tienen la capacidad de decidir qué tipo de contenido consideran problemático, lo que puede eludir las restricciones legales impuestas por los Estados. En contextos donde el Estado tiene limitaciones legales para intervenir, las plataformas pueden no estar sujetas a esas mismas restricciones.¹³ Esto puede generar una reacción por parte de los ciudadanos que sientan que la censura ejercida en línea vulnera sus derechos constitucionales o legales.

Un aspecto destacable de esta relación es el cambio que se ha dado en la legislación: ya no se centra tanto en definir el tipo de contenido problemático o el lenguaje que lo caracteriza, sino en señalar las responsabilidades de las plataformas, y supervisarlas en consecuencia. Esto permite que las propias empresas definan qué contenido debe ser regulado, y tengan un papel clave en establecer qué constituye un discurso o contenido problemático en un momento determinado¹⁴.

Todo esto ocurre en un entorno digital marcado por la tensión entre la necesidad de las plataformas de restringir contenidos considerados indeseables y, al mismo tiempo, maximizar la participación de los usuarios y el contenido generado por ellos.

La autorregulación representa una forma de control y censura que no depende directamente del Estado o del poder legislativo. Una de sus ventajas es su

¹² Tom Tyler, Matt Katsaros, Tracey Meares, and Sudhir Venkatesh, 'Social Media Governance: Can Social Media Companies Motivate Voluntary Rule Following Behaviour Among Their Users?' [2021] 17 Journal of Experimental Criminology 109.

¹³ Amelie Heldt, 'Let's Meet Halfway: Sharing New Responsibilities in a Digital Age' [2019] 9 Journal of Information Policy 336.

¹⁴ Natali Helberger, Jo Pierson, and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' [2018] 34 The Information Society 1.

capacidad de adaptación. Si la regulación de la seguridad en línea puede desarrollarse sin depender exclusivamente de marcos legales que definan, por ejemplo, qué es el discurso de odio, entonces se abre la posibilidad de una regulación más flexible, capaz de adaptarse a nuevas formas de contenido problemático.

Por otro lado, si la legislación únicamente determina **quién debe regular** sin especificar **qué contenido** debe ser regulado, el público puede llegar a percibir que las empresas están excediendo sus funciones e infringiendo derechos como la libertad de expresión. Aunque esta distancia entre las empresas y el Estado puede proteger a los gobiernos de las críticas por limitar la libre expresión, también puede dar lugar a la percepción de que el Estado **no está haciendo lo suficiente** para proteger a los ciudadanos frente al poder de las corporaciones.¹⁵

Gran parte de la investigación actual sobre la regulación de contenidos se ha centrado en la relación legal y regulatoria entre el Estado y las empresas, pero se ha prestado **menos atención a cómo el público percibe** tanto el contenido extremista en línea, como las responsabilidades del Estado y las respuestas de las redes sociales. En cuanto a quién debe asumir la responsabilidad de regular el contenido, las opiniones del público son diversas. Riedl et al. (2021) encontraron que las actitudes hacia la censura estatal o corporativa varían en función de cómo se valoren temas políticos fundamentales como la libertad de expresión y los derechos civiles. Esto también se refleja en las prácticas de moderación y regulación que aplican las plataformas, las cuales suelen responder tanto a las expectativas de los usuarios como a las demandas reales o supuestas del Estado.¹⁶

1.4 Precedentes internacionales en regulación de redes sociales

Ante la creciente preocupación por el impacto de las redes sociales en la democracia y la seguridad digital, varios países han implementado legislaciones pioneras para mitigar sus efectos negativos. Entre ellas destacan:

- **Reino Unido (Online Safety Act 2023):** Esta legislación obliga a las plataformas digitales a implementar medidas estrictas para proteger a los menores y combatir la desinformación, estableciendo sanciones para aquellas empresas que no cumplan con los estándares de seguridad digital.
- **Australia (Online Safety Amendment Act 2024):** Introduce una edad mínima para el uso de redes sociales y exige verificación de identidad obligatoria para todos los usuarios con el fin de combatir el acoso cibernético y garantizar la protección de menores en línea.
- **Vietnam (Decree 147/2024):** Requiere que todas las plataformas extranjeras que operen en el país tengan una presencia legal y respondan a

¹⁵ Reed and Henschke (n 22).

¹⁶ Martin Riedl et al, 'Who Is Responsible for Interventions against Problematic Comments? Comparing User Attitudes in Germany and the United States' [2021] 13 Policy & Internet 433.

los requerimientos del gobierno en materia de protección de datos y regulación de contenido.

Estos precedentes muestran la creciente tendencia a establecer regulaciones que protejan a los usuarios sin comprometer la innovación digital ni la libertad de expresión. Como indica Nyabola, "la consolidación de múltiples corporaciones digitales bajo una sola empresa matriz ha generado un modelo en el que los datos se comparten sin consentimiento informado de los usuarios", lo que refuerza la necesidad de regulaciones claras que limiten el uso indebido de la información personal.

Además, en el caso de Australia, la ley obliga a las plataformas a "implementar mecanismos que permitan a los padres controlar la actividad de sus hijos en redes sociales y recibir alertas sobre posibles riesgos". Estas disposiciones son relevantes para Colombia, donde el acceso irrestricto de menores a plataformas digitales ha expuesto a niños y adolescentes a diversas amenazas.

1.4.1 El caso australiano:

Australia cuenta con una de las legislaciones más avanzadas a nivel mundial para regular a las empresas de redes sociales y garantizar la seguridad en línea. Actualmente, el país aplica al menos tres enfoques legales distintos para controlar la publicación y difusión de contenido violento extremista, imágenes extremistas y discursos de odio. Estos incluyen: órdenes de eliminación bajo la Ley de Seguridad en Línea de 2021 (Online Safety Act 2021); órdenes específicas para retirar material violento atroz (AVM), establecidas en la División 474, Subdivisión H del Código Penal, aprobadas rápidamente tras los ataques a las mezquitas de Christchurch perpetrados por el australiano Brenton Tarrant; y disposiciones federales más recientes contenidas en la División HA del mismo código, orientadas a regular símbolos y saludos nazis tanto en línea como en espacios públicos, derivadas de las reformas introducidas por la Ley de Enmienda en Legislación Antiterrorista (Símbolos de Odio Prohibidos y Otras Medidas) de 2023.

La rápida proliferación y diversidad de enfoques para regular contenidos extremistas similares en línea ha complicado y ampliado significativamente el papel del Comisionado Federal de Seguridad en Línea (eSafety Commissioner) en Australia, al tiempo que impone una carga considerable tanto sobre las empresas privadas como sobre los individuos que actúan como proveedores de contenido y administradores de plataformas. Estos regímenes legales contemplan tanto responsabilidad civil como penal para personas y corporaciones que no cumplan con las órdenes de eliminación de contenido.

Resulta preocupante que algunas formas de responsabilidad, como las establecidas en el régimen de material violento atroz (AVM), se configuren de manera inusual, omitiendo pruebas requeridas en los estándares tradicionales del derecho penal federal —por ejemplo, presumiendo la culpabilidad si no se acata una orden de eliminación una vez notificada, sin necesidad de demostrar elementos de culpa.

Las tensiones entre los reguladores estatales australianos, como el eSafety Commissioner¹⁷, y empresas como X Corp, han derivado recientemente en litigios que han favorecido algunas de las libertades reivindicadas por estas plataformas, lo que ha complicado las expectativas del Gobierno australiano respecto a la aplicación extraterritorial de sus leyes. Algunas decisiones judiciales que han limitado el alcance de esa extraterritorialidad han generado vacíos regulatorios que permiten a los ciudadanos australianos seguir accediendo a contenidos bloqueados en el país mediante métodos alternativos como el uso de VPN.

Algunos recientes y preocupantes hechos violentos ocurridos en Australia —como el apuñalamiento en Bondi (no clasificado como acto terrorista) y el ataque en la iglesia de Wakeley (considerado incidente terrorista)— han avivado el debate público sobre cuál es el equilibrio adecuado entre la libertad de expresión, la libertad de las plataformas para regular su propio contenido, las demandas de los usuarios en redes sociales, la capacidad de respuesta de distintas plataformas frente a las autoridades y las preocupaciones de bienestar expresadas por gobiernos y grupos de víctimas. Estos eventos, junto con los litigios en curso, han puesto sobre la mesa cuestiones sobre cómo ofrecer información de seguridad en tiempo real durante incidentes violentos en desarrollo. Algunos expertos han cuestionado la idoneidad de los esquemas más recientes, en particular el régimen de Material Violento Atroz (AVM), así como la relación entre los distintos marcos regulatorios, incluyendo posibles redundancias no deseadas y diferencias en su aplicación.¹⁸

The Online Safety Act regime:

Esta ley entró en vigor el 23 de enero de 2023 con el objetivo de mejorar y promover la seguridad en línea de los australianos.¹⁹ **No solo establece la oficina del Comisionado Federal de Seguridad en Línea (eSafety Commissioner) y define diversas responsabilidades y procedimientos para la gestión de denuncias, sino que también establece expectativas básicas de seguridad en línea (y códigos de la industria), así como las obligaciones de reporte relacionadas con dichas expectativas o códigos.** Además, otorga al eSafety Commissioner la

¹⁷ Rachel Clun and Patrick Begley, 'Bondi Junction Stabbing as It Happened: Multiple Dead, Injured in Sydney's Eastern Suburbs; PM, NSW Police Commissioner Speak' Sydney Morning Herald (14 April 2024) <www.smh.com.au/national/nsw/bondi-junction-shooting-stabbings-live-updates-police-operation-in-sydney-s-eastern-suburbs-20240413-p5fjku.html> accessed 1 July 2024

¹⁸ Submission to the Parliamentary Joint Committee on Intelligence and Security, 'Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Bill 2023' <www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/HateSymbolsBill/Submissions> (Submission No 104, Charles Sturt University, 21 July 2021).

¹⁹ Section 3, Online Safety Act 2021 (Cth).

facultad de emitir notificaciones de eliminación de contenido, solicitando a personas o empresas que retiren publicaciones que muestren violencia extremista. El artículo 23(2) de la Ley de Seguridad en Línea establece que la aplicación de esta ley “se extiende a actos, omisiones, asuntos y situaciones ocurridas fuera de Australia”.

El ejercicio más reciente y de mayor perfil de las facultades del eSafety Commissioner para ordenar la eliminación de contenido se dio tras el apuñalamiento del obispo Mar Mari Emmanuel, ocurrido durante su sermón en una misa transmitida en vivo desde la iglesia asiria Christ the Good Shepherd en Wakeley, Sídney (Nueva Gales del Sur), la noche del 15 de abril de 2024. A raíz de este hecho, se inició una serie de procesos judiciales en la Corte Federal entre el eSafety Commissioner y X Corp, después de que esta última impugnara el uso de las facultades de eliminación de contenido ejercidas mediante una notificación emitida el 16 de abril de 2024²⁰, bajo el artículo 109 de la Ley de Seguridad en Línea de 2021 (Cth). Dicha notificación solicitaba la eliminación de un video de 11 segundos grabado desde la parte trasera de la iglesia, en el que se observa a un intruso acercándose al obispo, levantando el brazo derecho y golpeándolo varias veces con un movimiento descendente, lo que provoca la caída del obispo hacia atrás. Aunque el cuchillo no es claramente visible, se pueden escuchar las reacciones de los asistentes a la ceremonia.

Un día después del ataque, la Comisionada de Seguridad en Línea (eSafety Commissioner) emitió una notificación de remoción conforme al artículo 109 a varias empresas de redes sociales. Esto ocurrió tras la designación del hecho como un incidente terrorista por parte del Comisionado de Policía, en medio de escenas trágicas de un disturbio callejero que estalló frente a la iglesia la noche del incidente, el cual incluyó daños a vehículos policiales y agresiones a oficiales por parte de simpatizantes del obispo. La notificación de remoción señalaba: “Esta notificación de remoción se le entrega conforme al artículo 109 de la Ley y le exige tomar todas las medidas razonables para asegurar la eliminación del material de clase 1...”. La notificación hacía referencia a 65 URL de publicaciones en la plataforma X y también indicaba que:

El contenido es material de clase 1 conforme a la Ley de Seguridad en Línea de 2021 (Cth), por mostrar cuestiones de crimen, crueldad y violencia real de tal manera que ofende los estándares de moralidad, decencia y decoro generalmente aceptados por adultos razonables, en la medida en que probablemente sería clasificado como RC [Contenido Restringido].

El artículo 109 de la Ley de Seguridad en Línea establece la expectativa de que la remoción se lleve a cabo dentro de las 24 horas (o en un plazo mayor autorizado por la Comisionada de Seguridad en Línea). El artículo 12 de la misma ley define la remoción como: “el material se considera removido de un servicio de redes sociales, servicio electrónico relevante o servicio de internet designado si no es

²⁰ eSafety Commissioner v X Corp [2024] FCA 499.

accesible ni entregado a ninguno de los usuarios finales en Australia que utilicen dicho servicio”.²¹

Curiosamente, a medida que se desarrollaba el debate público y se alzaban fuertes críticas contra la notificación de remoción, incluyendo las del propietario de X Corp, Elon Musk, el obispo Mar Mari Emmanuel —quien se recuperaba tras haber sido apuñalado— hizo declaraciones públicas, reportadas ante la Corte Federal por X Corp, solicitando la publicación continua en línea del video del apuñalamiento.

Este caso internacional resalta la complejidad y urgencia de establecer marcos normativos robustos para la regulación de redes sociales, especialmente en situaciones donde el contenido difundido puede atentar contra la seguridad pública, la moralidad y los derechos fundamentales. La experiencia australiana demuestra cómo, ante hechos violentos o de interés nacional, las autoridades deben contar con herramientas legales claras y eficaces para exigir la remoción rápida de contenido nocivo.

En el contexto colombiano, donde el uso de redes sociales es masivo y creciente, el presente Proyecto de Ley busca justamente otorgar esas facultades a las entidades regulatorias nacionales, asegurando una respuesta oportuna frente a publicaciones que inciten al odio, la violencia o vulneren la dignidad humana, sin desconocer la importancia de proteger la libertad de expresión en un entorno digital cada vez más complejo.

Las herramientas más recientes en el conjunto de medidas regulatorias de redes sociales en Australia fueron aprobadas mediante legislación orientada a regular el uso, publicación y comercialización de símbolos nazis y el uso del saludo nazi: la Ley de Enmienda de Legislación Antiterrorista Referencial (Símbolos de Odio Prohibidos y Otras Medidas) de 2023 (Cth). La mayoría de las disposiciones recientemente creadas en la Subdivisión HA de la División 474 del Código Penal (Cth) entraron en vigor el 8 de enero de 2024 y, en lugar de autorizar a la Comisionada de Seguridad en Línea (eSafety Commissioner) para emitir notificaciones de remoción, esta subdivisión crea delitos relacionados con el “material extremista violento”, como el uso de servicios de telecomunicaciones para acceder, transmitir, solicitar, publicar o enlazar a dicho material. También se contempla el delito de posesión o control de material extremista violento.

El material extremista violento se define como una representación o descripción de violencia grave, la cual se refiere, conforme al artículo 100.1 del Código Penal (Cth), a actos de violencia terrorista, e incluye una variedad de acciones vinculadas a la violencia grave, tales como instrucción, apoyo o facilitación, asistencia, incitación, planificación o conspiración para actos intimidatorios. A diferencia de las

²¹ Tom Crowley, ‘Bishop Mar Mari Emmanuel Wants Footage of his Stabbing in Wakeley Church to Stay Online, Court Hears’ ABC News (24 April 2024) <www.abc.net.au/news/2024-04-24/bishop-emmanul-wants-stabbing-footageinjunction-extended/103764228> accessedido abril de 2025

disposiciones penales de la Subdivisión H de la División 474, estos delitos contienen elementos de culpabilidad claramente definidos que deben ser probados por los fiscales, y no se presumen automáticamente por hechos como el incumplimiento de notificaciones de remoción emitidas por la Comisionada de Seguridad en Línea.

3. FUNDAMENTOS JURÍDICOS

En Colombia, el uso del internet y las redes sociales ha adquirido una importancia creciente en la regulación jurídica, no solo por el impacto que tienen en la vida cotidiana, sino también por los riesgos que generan cuando se usan de manera indebida. El desarrollo normativo en esta área ha sido progresivo y responde a la necesidad de proteger derechos fundamentales como la libertad de expresión, la intimidad, el buen nombre y la protección de datos personales.

La **Constitución Política de Colombia** establece dos pilares fundamentales en esta materia: el artículo 15 garantiza el derecho a la intimidad personal y familiar, así como al buen nombre, y señala que todas las personas tienen derecho a conocer, actualizar y rectificar la información que sobre ellas se haya recopilado en bases de datos. A su vez, el artículo 20 consagra el derecho a la libertad de expresión, permitiendo a toda persona expresar y difundir libremente su pensamiento, opiniones e información, con la exigencia de veracidad e imparcialidad²².

Estas disposiciones generan una tensión natural entre dos derechos fundamentales: la expresión libre y la protección de la intimidad. En un entorno digital donde las opiniones, fotos, datos y comentarios circulan a gran velocidad, el Estado se ha visto obligado a intervenir mediante leyes específicas que buscan mitigar los riesgos y establecer límites jurídicos claros.

Una de las primeras respuestas legislativas frente a los peligros del entorno digital fue la **Ley 679 de 2001**, la cual previene y combate la explotación sexual de menores a través de internet. Esta norma promueve la autorregulación de los proveedores de servicios de internet para impedir la difusión de pornografía infantil, e impone deberes a empresas y entidades públicas en materia de prevención²³.

Posteriormente, con la **Ley 1266 de 2008** se reguló el manejo de información personal en bases de datos, estableciendo los principios del habeas data financiero

²² Congreso de Colombia. (1991). *Constitución Política de Colombia*. https://www.secretariassenado.gov.co/senado/basedoc/constitucion_politica_1991.html

²³ Congreso de Colombia. (2001). *Ley 679 de 2001*. Diario Oficial No. 44.509. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=18309>

y comercial, con el objetivo de proteger los derechos de los titulares de los datos frente al uso que de ellos hagan entidades públicas y privadas²⁴.

La **Ley 1273 de 2009** fue clave al modificar el Código Penal y reconocer la protección de los datos informáticos como un bien jurídico autónomo. Tipificó conductas como el acceso abusivo a sistemas, la interceptación de datos sin autorización, el daño informático y el uso de software malicioso²⁵.

En complemento, la **Ley 1341 de 2009** establece los principios para la organización de las Tecnologías de la Información y las Comunicaciones (TIC) y faculta al Estado a intervenir en este sector por razones de defensa nacional o seguridad pública²⁶.

El avance de las amenazas cibernéticas llevó también a promulgar la **Ley 1373 de 2009**, que refuerza las penas para delitos digitales y cierra vacíos legales existentes²⁷.

La protección de datos personales fue ampliada con la **Ley 1581 de 2012**, que introdujo principios generales sobre el tratamiento de datos y definió claramente los deberes de quienes manejan información personal, tanto en el sector público como en el privado²⁸.

En el ámbito técnico y de cooperación con las autoridades judiciales, el **Decreto 1704 de 2012** obliga a los proveedores de servicios a garantizar infraestructura que permita interceptaciones legales autorizadas por la Fiscalía, y establece la conservación de datos por un periodo mínimo de cinco años²⁹.

En el sector educativo, la **Ley 1620 de 2013** busca crear entornos escolares seguros, abordando también la prevención del ciberacoso, promoviendo la formación en derechos humanos y el uso responsable de medios digitales³⁰.

²⁴ Congreso de Colombia. (2008). *Ley 1266 de 2008*. Diario Oficial No. 47.219. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34306>

²⁵ Congreso de Colombia. (2009). *Ley 1273 de 2009*. Diario Oficial No. 47.223. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

²⁶ Congreso de Colombia. (2009). *Ley 1341 de 2009*. Diario Oficial No. 47.426. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37106>

²⁷ Congreso de Colombia. (2009). *Ley 1373 de 2009*. Diario Oficial No. 47.388. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37291>

²⁸ Congreso de Colombia. (2012). *Ley 1581 de 2012*. Diario Oficial No. 48.587. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

²⁹ Presidencia de la República de Colombia. (2012). *Decreto 1704 de 2012*. Diario Oficial No. 48.518. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49718>

³⁰ Congreso de Colombia. (2013). *Ley 1620 de 2013*. Diario Oficial No. 48.733. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52379>

Finalmente, la **Ley Estatutaria 1621 de 2013** regula las actividades de inteligencia y contrainteligencia del Estado, estableciendo parámetros legales para la recolección de información, con el objetivo de salvaguardar la seguridad nacional sin vulnerar los derechos fundamentales³¹.

En conjunto, este cuerpo normativo refleja el esfuerzo del Estado colombiano por garantizar que el entorno digital sea un espacio seguro, donde el ejercicio de la libertad de expresión no se convierta en una herramienta para dañar la honra o invadir la intimidad de los demás, y donde el avance tecnológico no supere la capacidad de proteger los derechos fundamentales.

2.1 Jurisprudencia relevante sobre el uso de internet y redes sociales en Colombia

El desarrollo jurisprudencial en Colombia ha sido esencial para interpretar el alcance de los derechos fundamentales en entornos digitales. Aunque la Constitución garantiza tanto la libertad de expresión como el derecho a la intimidad, el buen nombre y el habeas data, la Corte Constitucional ha establecido que estos derechos no son absolutos y deben armonizarse según el contexto de cada caso.

Uno de los primeros precedentes clave es la **Sentencia T-260 de 2012**, donde se protegió el derecho a la intimidad de una menor de edad. En este caso, la Corte consideró que la creación de una cuenta de Facebook por parte del padre, sin el consentimiento de su hija, implicaba una vulneración a su derecho al libre desarrollo de la personalidad. El tribunal sostuvo que, incluso con buenas intenciones, los padres no pueden exponer a sus hijos en redes sociales sin su autorización, especialmente cuando esa exposición digital compromete su autonomía futura³².

La **Sentencia T-050 de 2016** reafirma que la libertad de expresión tiene límites cuando colisiona con el derecho al buen nombre. En este fallo, la Corte analizó publicaciones en redes sociales que afectaban la reputación de un tercero. El tribunal aclaró que, si bien internet permite una democratización de la opinión, esa libertad debe ejercerse de forma responsable, sin recurrir al insulto o a la desinformación que cause daño injustificado a otro ciudadano³³.

En la **Sentencia T-145 de 2016**, el alto tribunal trató directamente el tema del derecho al olvido digital. Una persona solicitó la eliminación de información personal desactualizada y perjudicial publicada en línea. La Corte estableció que

³¹ Congreso de Colombia. (2013). *Ley 1621 de 2013*. Diario Oficial No. 48.749. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52458>

³² Corte Constitucional de Colombia. (2012). *Sentencia T-260 de 2012*. M.P. Humberto Antonio Sierra Porto. <https://www.corteconstitucional.gov.co/relatoria/2012/t-260-12.htm>

³³ Corte Constitucional de Colombia. (2016). *Sentencia T-050 de 2016*. M.P. Gloria Stella Ortiz Delgado. <https://www.corteconstitucional.gov.co/relatoria/2016/t-050-16.htm>

la permanencia indefinida de ciertos contenidos en internet puede afectar el proyecto de vida de las personas, sobre todo si carecen de relevancia actual o interés público. Este pronunciamiento introdujo en el contexto colombiano el criterio de ponderación entre memoria digital e interés social de la información³⁴.

La **Sentencia T-277 de 2018** profundizó en la responsabilidad de los medios de comunicación digitales. La Corte señaló que si bien estos medios gozan de protección constitucional, deben verificar la veracidad de la información y evitar el daño a los derechos fundamentales de las personas mencionadas, en especial cuando el contenido se publica en entornos que amplifican su difusión, como redes sociales o portales web³⁵.

Finalmente, la **Sentencia SU-274 de 2019** unificó la jurisprudencia sobre el derecho al olvido y estableció que los motores de búsqueda pueden ser requeridos para desindexar enlaces cuando la información difundida, aunque veraz, haya perdido relevancia pública, sea obsoleta o cause un daño desproporcionado. Esta sentencia marcó un hito al reconocer que el control de la huella digital es parte del ejercicio de los derechos fundamentales en la era de la información³⁶.

Estos pronunciamientos reflejan una evolución coherente del derecho colombiano hacia la protección de la dignidad humana en el entorno digital. La Corte ha adoptado un enfoque garantista, basado en el principio de proporcionalidad, para asegurar que el ejercicio de la libertad de expresión en redes sociales y plataformas digitales no implique una afectación injustificada de otros derechos.

4. CONFLICTO DE INTERESES

El artículo 3 de la Ley 2003, promulgada el 19 de noviembre de 2019, introduce una modificación al artículo 291 de la Ley 5 de 1992.

Esta modificación establece que los autores y ponentes de proyectos de ley deben incluir en la sección de justificación de sus propuestas un apartado en el cual se detalle las situaciones o incidentes que pudieran dar lugar a conflictos de interés para los miembros del Congreso durante el proceso de debate y votación de dichas iniciativas legislativas.

En este sentido, con el fin de ilustrar en el análisis frente a los posibles impedimentos que podrían derivar en conflictos de intereses producto de la

³⁴ Corte Constitucional de Colombia. (2016). *Sentencia T-145 de 2016*. M.P. Gloria Stella Ortiz Delgado. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=72327>

³⁵ Corte Constitucional de Colombia. (2018). *Sentencia T-277 de 2018*. M.P. Alejandro Linares Cantillo. <https://www.corteconstitucional.gov.co/relatoria/2018/t-277-18.htm>

³⁶ Corte Constitucional de Colombia. (2019). *Sentencia SU-274 de 2019*. M.P. Alberto Rojas Ríos. <https://img.lpderecho.pe/wp-content/uploads/2022/05/Sentencia-SU274-19-Colombia-LPDerecho.pdf>

actividad legislativa realizada, se citarán textualmente los criterios determinados en el artículo 1 de la ley 2003 de 2019:

“ARTÍCULO 1o. *El artículo 286 de la Ley 5 de 1992 quedará así:*

Artículo 286. Régimen de conflicto de interés de los congresistas. *Todos los congresistas deberán declarar los conflictos de intereses que pudieran surgir en ejercicio de sus funciones.*

Se entiende como conflicto de interés una situación donde la discusión o votación de un proyecto de ley o acto legislativo o artículo, pueda resultar en un beneficio particular, actual y directo a favor del congresista.

a) Beneficio particular: aquel que otorga un privilegio o genera ganancias o crea indemnizaciones económicas o elimina obligaciones a favor del congresista de las que no gozan el resto de los ciudadanos. Modifique normas que afecten investigaciones penales, disciplinarias, fiscales o administrativas a las que se encuentre formalmente vinculado.

b) Beneficio actual: aquel que efectivamente se configura en las circunstancias presentes y existentes al momento en el que el congresista participa de la decisión.

c) Beneficio directo: aquel que se produzca de forma específica respecto del congresista, de su cónyuge, compañero o compañera permanente, o parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil.

Para todos los efectos se entiende que no hay conflicto de interés en las siguientes circunstancias:

a) Cuando el congresista participe, discuta, vote un proyecto de ley o de acto legislativo que otorgue beneficios o cargos de carácter general, es decir cuando el interés del congresista coincide o se fusione con los intereses de los electores.

b) Cuando el beneficio podría o no configurarse para el congresista en el futuro.

c) Cuando el congresista participe, discuta o vote artículos de proyectos de ley o acto legislativo de carácter particular, que establezcan sanciones o disminuyan beneficios, en el cual, el congresista tiene un interés particular, actual y directo. El voto negativo no constituirá conflicto de interés cuando mantiene la normatividad vigente.

d) Cuando el congresista participe, discuta o vote artículos de proyectos de ley o acto legislativo de carácter particular, que regula un sector económico en el cual el congresista tiene un interés particular, actual y directo, siempre y cuando no genere beneficio particular, directo y actual.

e) <Literal INEXEQUIBLE>

f) Cuando el congresista participa en la elección de otros servidores públicos mediante el voto secreto. Se exceptúan los casos en que se presenten inhabilidades referidas al parentesco con los candidatos.

PARÁGRAFO 1o. *Entiéndase por conflicto de interés moral aquel que presentan los congresistas cuando por razones de conciencia se quieran apartar de la discusión y votación del proyecto.*

PARÁGRAFO 2o. *Cuando se trate de funciones judiciales, disciplinarias o fiscales de los congresistas, sobre conflicto de interés se aplicará la norma especial que rige ese tipo de investigación.*

PARÁGRAFO 3o. *Igualmente se aplicará el régimen de conflicto de intereses para todos y cada uno de los actores que presenten, discutan o participen de cualquier iniciativa legislativa, conforme al artículo 140 de la Ley 5 de 1992 (...).*

En este contexto y en estricto cumplimiento de la legislación vigente, en mi calidad de autor de este proyecto, considero que este no genera conflictos de interés con el suscrito. Esto se debe a que se trata de una iniciativa de interés general, aplicable de manera equitativa a todos, que puede coincidir con los intereses de los electores en su conjunto.

En otras palabras, no se presenta una situación específica que resulte en un beneficio personal ni se percibe un beneficio actual en las circunstancias actuales.

Además, no existe la posibilidad de un beneficio directo que pueda beneficiar de manera específica al congresista, a sus cónyuges, parejas permanentes o parientes hasta el segundo grado de parentesco por consanguinidad, afinidad o civil.

Sin perjuicio de lo anterior, se debe tener en cuenta que la descripción de los posibles conflictos de interés que se puedan presentar frente al trámite del presente proyecto de ley, no exime del deber del Congresista que, en su esfera privada, identifique causales adicionales que a su juicio considere pertinentes y exponerlas durante el trámite correspondiente.

En estos términos dejo a consideración del Congreso de la República esta iniciativa para que sea discutida, mejorada y aprobada en beneficio de los colombianos y

colombianas que ven afectada su vida crediticia por el hecho de buscar dignificación en el estudio superior.

5. IMPACTO FISCAL DE LA INICIATIVA:

Respecto del concepto impacto fiscal que los proyectos de ley pudieran generar, la Corte ha dicho:

“Las obligaciones previstas en el artículo 7° de la Ley 819 de 2003 constituyen un parámetro de racionalidad legislativa, que está encaminado a cumplir propósitos constitucionalmente valiosos, entre ellos el orden de las finanzas públicas, la estabilidad macroeconómica y la aplicación efectiva de las leyes. Esto último en tanto un estudio previo de la compatibilidad entre el contenido del proyecto de ley y las proyecciones de la política económica, disminuye el margen de incertidumbre respecto de la ejecución material de las previsiones legislativas. El mandato de adecuación entre la justificación de los proyectos de ley y la planeación de la política económica, empero, no puede comprenderse como un requisito de trámite para la aprobación de las iniciativas legislativas, cuyo cumplimiento recaiga exclusivamente en el Congreso.

Lo anterior, en tanto (i) el Congreso carece de las instancias de evaluación técnica para determinar el impacto fiscal de cada proyecto, la determinación de las fuentes adicionales de financiación y la compatibilidad con el marco fiscal de mediano plazo; y (ii) aceptar una interpretación de esta naturaleza constituiría una carga irrazonable para el legislador y otorgaría un poder correlativo de veto al Ejecutivo, a través del Ministerio de Hacienda, respecto de la competencia del Congreso para hacer las leyes. Un poder de este carácter, que involucra una barrera en la función constitucional de producción normativa, se muestra incompatible con el balance entre los poderes públicos y el principio democrático. Si se considera dicho mandato como un mecanismo de racionalidad legislativa, su cumplimiento corresponde inicialmente al Ministerio de Hacienda y Crédito Público, una vez el Congreso haya valorado, mediante las herramientas que tiene a su alcance, la compatibilidad entre los gastos que genera la iniciativa legislativa y las proyecciones de la política económica trazada por el Gobierno. (...). El artículo 7° de la Ley 819/03 no puede interpretarse de modo tal que la falta de concurrencia del Ministerio de Hacienda y Crédito Público dentro del proceso legislativo, afecte la validez constitucional del trámite respectivo”. (Sentencia C-315 de 2008).

Como lo ha resaltado la Corte, si bien compete a los miembros del Congreso la responsabilidad de estimar y tomar en cuenta el esfuerzo fiscal que el proyecto bajo estudio puede implicar para el erario público, es claro que es el Poder Ejecutivo, y al interior de aquel, el Ministerio de Hacienda y Crédito Público, el que dispone de los elementos técnicos necesarios para valorar correctamente ese impacto, y a partir de ello, llegado el caso, demostrar a los miembros del órgano legislativo la inviabilidad financiera de la propuesta que se estudia.

Sin embargo, frente a las disposiciones propuestas en el presente proyecto de Ley, consideramos que las mismas no generan un impacto fiscal adicional, pues en las mismas no existe la ordenación de gastos ni la generación de beneficios tributarios.

6. CONCLUSIONES

La irrupción masiva de las redes sociales en la vida cotidiana de los colombianos ha planteado desafíos inéditos para el orden jurídico, la seguridad ciudadana y la garantía efectiva de los derechos fundamentales en entornos digitales. El presente Proyecto de Ley constituye una respuesta normativa integral, urgente y pertinente frente a los vacíos legales que actualmente dificultan la supervisión y responsabilidad de las plataformas digitales en Colombia.

Desde una perspectiva constitucional, la libertad de expresión consagrada en el artículo 20 de la Constitución Política no puede entenderse como un derecho absoluto. Tal como ha reiterado la Corte Constitucional en sentencias como la **T-050 de 2016**, **T-260 de 2012** y **SU-274 de 2019**, este derecho debe armonizarse con otros de igual jerarquía como la intimidad, el buen nombre, la honra, el habeas data y el libre desarrollo de la personalidad. En este sentido, regular las redes sociales no es una forma de censura, sino una acción estatal necesaria para garantizar el ejercicio de los derechos en condiciones de equidad, dignidad y seguridad jurídica.

El proyecto propone medidas que tienen respaldo en la normativa vigente y desarrollan estándares reconocidos en el derecho comparado. La obligación de verificación de identidad para usuarios no solo combate la suplantación y la comisión de delitos cibernéticos —como lo ha evidenciado la aplicación de normas como la **Ley 1273 de 2009**—, sino que se alinea con prácticas internacionales en países como Australia y Reino Unido, donde la regulación digital ha sido fortalecida para enfrentar fenómenos como el extremismo, la explotación infantil, la manipulación política y la violencia en línea.

Asimismo, el enfoque preventivo en la protección de menores de edad responde a los principios establecidos en la **Ley 679 de 2001** y la **Ley 1620 de 2013**, reconociendo que los niños y adolescentes son sujetos de especial protección constitucional. Permitir el acceso irrestricto de menores a redes sociales sin mecanismos eficaces de control no solo los expone a riesgos como el ciberacoso o la explotación, sino que transgrede el deber del Estado de garantizar su desarrollo integral.

En cuanto a la protección de datos personales, la propuesta legislativa fortalece el marco del **habeas data** establecido en las leyes **1266 de 2008** y **1581 de 2012**, exigiendo consentimiento informado y transparencia en el manejo de la información por parte de las plataformas. Este es un elemento esencial en un entorno digital donde la comercialización de datos se ha convertido en el núcleo del modelo de negocio de muchas empresas tecnológicas.

Adicionalmente, al asignar competencias claras a la Superintendencia de Industria y Comercio como autoridad reguladora y sancionatoria, el proyecto no solo garantiza la aplicación efectiva de las disposiciones, sino que asegura un sistema institucional robusto con capacidad de control y seguimiento, lo cual es indispensable para materializar los principios de legalidad, eficacia y responsabilidad.

La jurisprudencia constitucional y el derecho internacional respaldan un enfoque de regulación proporcional, progresiva y basada en el interés general. Este proyecto de ley no impone restricciones arbitrarias, sino que busca construir un ecosistema digital más seguro, transparente y respetuoso de los derechos, promoviendo a la vez una cultura de ciudadanía digital responsable.

En conclusión, el presente Proyecto de Ley representa una iniciativa legislativa coherente con los desafíos contemporáneos del país, fundada en principios constitucionales, en estándares internacionales y en el interés superior de los usuarios. Su aprobación fortalecerá el Estado de Derecho en el entorno digital y permitirá que las redes sociales continúen siendo espacios de interacción, participación y libertad, dentro de un marco que prioriza la protección de la persona humana, el orden democrático y la convivencia pacífica.

Cordialmente,

GERMÁN ROGELIO ROZO ANIS

Representante a la Cámara
Departamento de Arauca