Bogotá D.C., 24 de Noviembre de 2026

Doctor
MIGUEL ANGEL SÁNCHEZ VÁZQUEZ
Secretario General
Cámara de Representantes

Ref.: Radicación Proyecto de Ley Estatutaria N° 522 de 2026
"*"Por medio de la cual se reconoce y desarrolla el derecho a la identidad digital, se establecen mecanismos de verificación de identidad en plataformas digitales, se protege el anonimato frente al público, se fortalecen las herramientas para la prevención e investigación de delitos cometidos mediante entornos digitales y se dictan otras disposiciones."*"

Cordial saludo,

En nuestra condición de congresistas y en cumplimiento de los artículos 150 y 154 de la Constitución Política, así como de los artículos 139, 140 y 145 de la Ley 5 de 1992, nos disponemos a radicar ante la honorable Cámara de Representantes el presente proyecto de ley.
De los honorables congresistas,

MIGUEL ÁNGEL PINTO RUEDA Representante a la Cámara	**DANIEL BRICEÑO** Representante a la Cámara Bogotá ***Coautor***

Autor Departamento de Santander	
MAURICIO TORO ORJUELA Representante a la Cámara Bogotá ***Coautor***	**Eimy Suárez González** Representante a la Cámara Norte de Santander ***Coautor***
JAIME ARIZABALETA FAJARDO Representante a la Cámara Departamento del Valle del Cauca Partido Centro Democrático	**JUAN DAVID LONDOÑO ARANGO** Representante a la Cámara Departamento de Vichada Partido de la U
MATEO HIDALGO MONTOYA Representante a la Cámara Caldas ***Coautor***	**MARTHA ISABEL RUIZ SOLERA** Representante a la Cámara Por Córdoba ***Coautor***

PROYECTO DE LEY ESTATUTARIA N.° 522 DE 2026

"Por medio de la cual se reconoce y desarrolla el derecho a la identidad digital, se establecen mecanismos de verificación de identidad en plataformas digitales, se protege el anonimato frente al público, se fortalecen las herramientas para la prevención e investigación de delitos cometidos mediante entornos digitales y se dictan otras disposiciones."

EL CONGRESO DE COLOMBIA

DECRETA:

Título I. Disposiciones Generales

Artículo 1. Objeto. La presente ley tiene por objeto reconocer y desarrollar el derecho a la identidad digital de las personas, establecer mecanismos de verificación de identidad aplicables a los proveedores de redes sociales y plataformas digitales que operen en Colombia, proteger el anonimato frente al público, y fortalecer las herramientas institucionales para la prevención, investigación y sanción de delitos cometidos a través de entornos digitales, incluyendo la suplantación de identidad, el acoso, la extorsión, el fraude, el grooming, la explotación sexual de niños, niñas y adolescentes, y la manipulación coordinada de la opinión pública mediante cuentas automatizadas o inauténticas.

Artículo 2. Ámbito de aplicación. Las disposiciones de la presente ley se aplicarán a las personas naturales y jurídicas usuarias de redes sociales y plataformas digitales ubicadas en el territorio nacional, y a los proveedores de redes sociales y plataformas digitales, nacionales o extranjeros, que permitan la creación de cuentas o el acceso a sus servicios por parte de usuarios ubicados en Colombia, en los términos del Título IV de la presente ley.

Para efectos de esta ley, se entiende que un proveedor ofrece una red social o plataforma digital sujeta a verificación de identidad cuando su función principal consiste en permitir que los usuarios generen contenido o interactúen entre sí de forma visible para otros usuarios o para el público en general. No quedan comprendidos, por la sola prestación de estas funciones, los servicios de mensajería privada punto a punto, los marketplaces y plataformas transaccionales o de pagos, los servicios de comercio electrónico B2B, las herramientas de productividad o colaboración empresarial, los videojuegos sin funcionalidades de interacción social masiva, ni las comunidades privadas cerradas, por tratarse de servicios de naturaleza transaccional o comercial y no de interacción pública; el riesgo de fraude propio de esas actividades se atiende mediante los regímenes de protección al consumidor y prevención del fraude que les resulten aplicables, y no mediante la presente ley. Dichos proveedores quedarán sujetos a esta ley, únicamente

miguel.pinto@camara.gov.co • Capitolio Nacional, Segundo Piso.
@rep.miguelpintorueda @MiguelPintoRep

respecto de la funcionalidad correspondiente, cuando habiliten difusión pública de contenido, monetización o publicidad en los términos del artículo 8° de la presente ley.

Artículo 3. Principios. La aplicación de la presente ley se regirá por los siguientes principios:

a) Proporcionalidad: las medidas de verificación e identificación se limitarán a lo estrictamente necesario para cumplir la finalidad de la presente ley.

b) Minimización de datos: solo se recolectará la información indispensable para la verificación de identidad.

c) Finalidad: la información recolectada no podrá usarse para propósitos distintos de los previstos en esta ley.

d) Reserva y confidencialidad: la información de identidad verificada tiene carácter reservado frente al público.

e) Debido proceso: el acceso de las autoridades a la información de identidad estará sujeto a control judicial.

f) No discriminación: los mecanismos de verificación serán accesibles y no podrán generar barreras injustificadas de acceso a las plataformas digitales.

Artículo 4. Definiciones. Para efectos de la presente ley se entiende por:

Identidad digital: conjunto de atributos, credenciales, perfiles y datos que permiten individualizar a una persona natural en los entornos digitales.

Anonimato frente al público: la facultad de toda persona de interactuar en plataformas de redes sociales bajo un seudónimo, alias o nombre distinto de su nombre civil, sin que dicha identidad civil sea conocida por los demás usuarios ni por terceros no autorizados por el titular.

Verificación de identidad: proceso mediante el cual un proveedor de redes sociales o plataformas digitales constata, a través de documentos oficiales u otros mecanismos idóneos, que una cuenta corresponde a una persona natural o jurídica determinada e identificable.

Proveedor de redes sociales o plataformas digitales: persona natural o jurídica que administra u opera una red social, aplicación o plataforma digital que permite a los usuarios crear cuentas, generar contenido o interactuar entre sí de forma visible para otros usuarios o para el público en general, en los términos y con las exclusiones previstas en el artículo 2° de la presente ley.

Proveedor de gran escala: proveedor de redes sociales o plataformas digitales que cuente, en al menos una de ellas, con tres millones (3.000.000) o más de usuarios activos mensuales promedio en el territorio nacional, según el reporte que presente ante la

autoridad y la metodología que defina la reglamentación. Se consideran, en todo caso, proveedores de gran escala Meta (Facebook e Instagram), TikTok, X (antes Twitter) y Google (YouTube).

Cuenta inauténtica o automatizada (bot): cuenta gestionada total o parcialmente por sistemas automatizados y/o que oculta o falsea la identidad de su operador con el propósito de simular la participación de una persona real.

Autoridad competente: la Fiscalía General de la Nación, las autoridades judiciales y las demás entidades públicas facultadas por la Constitución y la ley para investigar delitos o proteger derechos fundamentales.

Título II. Del Derecho a la Identidad Digital y del Anonimato Frente al Público

Artículo 5. Derecho a la identidad digital. Toda persona tiene derecho a construir, desarrollar y proteger su identidad digital, así como a la autodeterminación informativa sobre los datos que la componen, de conformidad con el artículo 15 de la Constitución Política y la Ley 1581 de 2012.

Artículo 6. Anonimato frente al público. Toda persona podrá utilizar seudónimos, alias, nombres artísticos o cualquier otra forma legítima de identificación pública dentro de las redes sociales, sin que ello la exima del cumplimiento de la obligación de verificación de identidad prevista en el Título III de la presente ley. El ejercicio del anonimato frente al público es una manifestación del derecho a la libertad de expresión y no podrá ser restringido por los proveedores de redes sociales y plataformas digitales; sin embargo, no es absoluto y podrá ser limitado por las autoridades competentes, de conformidad con la Constitución y la ley. Lo anterior no exime a los proveedores del cumplimiento de los deberes de identificación que les sean exigibles en virtud de otros regímenes legales aplicables a su actividad, tales como la protección al consumidor en el comercio electrónico (Ley 1480 de 2011, artículo 50).

Artículo 7. Prohibición de divulgación pública de la identidad verificada. Los proveedores de redes sociales y plataformas digitales no podrán revelar, publicar ni poner en conocimiento de otros usuarios o de terceros la identidad civil verificada de un usuario que opere bajo seudónimo, salvo: (i) por solicitud expresa y voluntaria del titular; (ii) por orden de autoridad judicial competente; o (iii) por requerimiento de la Fiscalía General de la Nación en el marco de una investigación penal o, en los casos de urgencia, de las autoridades facultadas por el artículo 15°, de conformidad con el Título V de la presente ley.

Parágrafo 1°. En los supuestos previstos en este artículo, la información y la documentación privadas del usuario recolectadas para efectos de la verificación de identidad solo se entregarán, según corresponda, al titular o a los destinatarios que este designe expresamente, a la autoridad judicial que profirió la orden o a la autoridad que formuló el requerimiento, y se limitarán a lo estrictamente necesario para la finalidad de la

solicitud, la orden o el requerimiento. En ningún caso podrán compartirse ni divulgarse a otros terceros, de conformidad con los artículos 11°, 12° y 16° de la presente ley.

Título III. De la Verificación de Identidad en Plataformas Digitales

Artículo 8. Obligación de verificación de identidad. Los proveedores de redes sociales y plataformas digitales sujetos al ámbito de aplicación de la presente ley deberán verificar la identidad de las personas naturales que creen o administren cuentas en su plataforma, con independencia del número de cuentas que una misma persona posea, conforme al siguiente esquema gradual:

1. Verificación previa obligatoria. El proveedor deberá completar la verificación de identidad prevista en el artículo 9° de la presente ley antes de habilitar cualquiera de las siguientes funcionalidades:

   a. La percepción de ingresos, monetización, donaciones o cualquier contraprestación económica a través de la plataforma;

   b. La contratación, pauta o difusión de publicidad o de contenido comercial pagado;

   c. La difusión de contenido, mediante herramientas de promoción, amplificación algorítmica o pauta paga del proveedor, a audiencias que superen los umbrales de alcance que determine la reglamentación (no aplica al alcance orgánico obtenido sin promoción o amplificación activa del proveedor);

   d. La creación o administración de cuentas por parte de niños, niñas y adolescentes, salvo lo previsto en el artículo 10° de la presente ley.

2. Verificación por riesgo. El proveedor deberá exigir la verificación de identidad prevista en el artículo 9° y podrá restringir el uso de la cuenta hasta que aquella se complete, cuando existan indicios objetivos y documentables de: a. Suplantación de la identidad de un tercero; b. Operación automatizada o inauténtica en los términos del artículo 4° de la presente ley; c. Utilización de la cuenta para la comisión de alguna de las conductas señaladas en el artículo 1° de la presente ley.

3. Régimen general. Respecto de las cuentas no comprendidas en los numerales anteriores, los proveedores deberán mantener, como mínimo, un atributo de identificación verificado que permita individualizar al titular ante requerimiento de autoridad competente en los términos del Título V de la presente ley. Para estas cuentas no deberá exigirse la recolección de imágenes de documentos de identidad ni de datos biométricos.

Parágrafo 1°. La verificación de identidad prevista en este artículo no implica en ningún caso la identificación pública del usuario ante los demás usuarios de la plataforma ni ante terceros, de conformidad con los artículos 6° y 7° de la presente ley.

Parágrafo 2°. Los proveedores no podrán condicionar a la verificación de identidad el acceso a contenidos ni la navegación que no implique la creación o administración de una cuenta.

Parágrafo 3°. La reglamentación definirá los umbrales, criterios e indicadores de que trata este artículo atendiendo a los principios de proporcionalidad y minimización de datos previstos en el artículo 3°, precisando el indicador de alcance aplicable, el período de medición, los tipos de cuenta o funcionalidad cubiertos y las excepciones a que haya lugar, y podrá establecer criterios diferenciados para los proveedores que no sean de gran escala, en función de su capacidad técnica, operativa y financiera. Estos criterios podrán ajustar los mecanismos de verificación, pero no eximirán del régimen general del numeral 3 ni ampliarán los plazos del parágrafo transitorio.

Parágrafo 4°. Cuando el proveedor se encuentre sujeto a un régimen de debida diligencia de identificación de clientes equivalente al previsto en este artículo, en virtud de su sujeción al régimen de prevención de lavado de activos y financiación del terrorismo (SARLAFT) bajo supervisión de la Superintendencia Financiera de Colombia u otra autoridad competente, se entenderá cumplida la obligación de verificación previa prevista en el numeral 1, literal a., respecto de las cuentas ya verificadas bajo dicho régimen.

Parágrafo 5°. El proveedor que haya implementado razonablemente los mecanismos de verificación de identidad exigidos por esta ley y su reglamentación no será responsable cuando un usuario eluda dichos mecanismos mediante documentos o atributos falsificados, sin perjuicio de la responsabilidad que corresponda al autor de la falsificación.

Parágrafo 6°. Cuando la cuenta corresponda a una persona jurídica, la verificación de identidad comprenderá a la persona jurídica titular y a su representante legal, además de la persona natural que cree o administre la cuenta, mediante los documentos y registros públicos que defina la reglamentación (como el certificado de existencia y representación legal, el registro tributario o sus equivalentes en el país de origen). Esta verificación no implica la divulgación pública de los datos personales del representante legal ni de la persona natural responsable de la cuenta.

Parágrafo transitorio. Los proveedores de gran escala contarán con doce (12) meses para dar cumplimiento a lo previsto en el numeral 1, y con veinticuatro (24) meses para lo previsto en los numerales 2 y 3. Los demás proveedores contarán con doce (12) meses adicionales a esos plazos.

Estos plazos se contarán desde la expedición de la reglamentación o, a más tardar, desde el vencimiento del término previsto en el artículo 19°.

La condición de proveedor de gran escala se determinará, conforme al artículo 4°, a la fecha en que comiencen a contarse los plazos.

Artículo 9. Mecanismos de verificación. La verificación de identidad deberá realizarse, por lo menos, mediante la validación de la cédula de ciudadanía, la cédula de extranjería,

el pasaporte, u otros mecanismos tecnológicos equivalentes que garanticen un nivel de seguridad y confiabilidad razonable, como las herramientas de atestación de atributos (mayoría de edad, unicidad de la persona, entre otros) utilizables sobre la infraestructura de la Registraduría Nacional del Estado Civil, los cuales permitan constatar dichos atributos sin que el proveedor reciba, almacene o tenga acceso al documento de identidad o a los datos biométricos del usuario, en los términos que defina la reglamentación.

Alternativamente, la verificación prevista en este artículo podrá realizarse a través de prestadores de servicios de confianza digital, acreditados ante el Ministerio de Tecnologías de la Información y las Comunicaciones o el organismo de acreditación que este designe, que operen de forma interoperable con estándares abiertos de identidad digital (tales como credenciales verificables o documentos de identidad móviles), sin que ello suponga una dependencia exclusiva de la infraestructura de la Registraduría Nacional del Estado Civil.

La reglamentación podrá exigir mecanismos de verificación basados en pruebas de vida en los casos de mayor riesgo (como la monetización de la cuenta, la publicidad pagada, la difusión amplificada de contenido o los indicios de suplantación de identidad u operación inauténtica), sin que el proveedor reciba o almacene datos biométricos del usuario.

En todo caso, el proveedor deberá ofrecer, en especial para personas con discapacidad, adultos mayores o usuarios con limitaciones de conectividad o de dispositivo, un mecanismo alternativo no biométrico que garantice un nivel de seguridad equivalente, tales como: a) la atestación de atributos sobre la infraestructura de la Registraduría Nacional del Estado Civil; b) las credenciales verificables o los documentos de identidad móviles de prestadores de servicios de confianza digital acreditados; o c) la verificación presencial en los puntos de atención que defina la reglamentación.

Asimismo, el proveedor deberá disponer, sin costo para el usuario, de un mecanismo interno de apelación del resultado de la verificación y de un canal de comunicación accesible para atender las caídas, fallas o errores del proceso de verificación, incluidos los rechazos indebidos. Las solicitudes presentadas por estos medios serán atendidas por una persona natural y no podrán resolverse exclusivamente mediante sistemas automatizados, dentro del plazo razonable que defina la reglamentación, sin perjuicio de los derechos del titular conforme a la Ley 1581 de 2012.

Parágrafo 1°. Se entenderá cumplida la obligación de verificación prevista en este artículo respecto de quien acredite el cumplimiento de las obligaciones de verificación de identidad y gestión de evidencia establecidas en la Ley Estatutaria 2573 de 2026, en los términos y plazos allí previstos.

La reglamentación establecerá los mecanismos de interoperabilidad técnica y armonización regulatoria necesarios entre las obligaciones de esta ley y las de la Ley Estatutaria 2573 de 2026, de forma que un mismo proceso de verificación no genere cargas de cumplimiento duplicadas.

Artículo 10. Verificación de cuentas de menores de edad. La creación de cuentas por parte de menores de edad requerirá, además de la verificación de la identidad del menor, la verificación de la identidad de un adulto responsable que declare bajo gravedad de juramento ejercer la representación legal del menor y señale su autorización expresa, en los términos que defina la reglamentación, sin perjuicio del interés superior del menor y del derecho progresivo a la participación consagrados en la Ley 1098 de 2006.

La verificación prevista en este artículo se implementará de manera gradual y proporcional al nivel de riesgo del servicio o funcionalidad ofrecidos, conforme al modelo de verificación de edad basado en riesgo, minimización de datos y neutralidad tecnológica previsto en la Ley 2489 de 2025 y el Decreto 769 de 2026, o las normas que los modifiquen o sustituyan. En los servicios o funcionalidades de bajo riesgo, la reglamentación podrá disponer mecanismos de verificación de edad que no impliquen la verificación adicional de identidad de un adulto responsable.

La reglamentación reconocerá como válidos los mecanismos de verificación parental o de estimación de edad que cuenten con validación técnica internacional y sean interoperables con los estándares previstos en la Ley 2489 de 2025 y el Decreto 769 de 2026, sin que ello exima del cumplimiento de los principios de proporcionalidad y minimización de datos previstos en el artículo 3°.

Artículo 11. Conservación y protección de la información de verificación. Los datos e información recolectados para efectos de la verificación de identidad serán tratados conforme a la Ley 1581 de 2012 y demás normas que regulan la protección de datos personales. Concluido el proceso de verificación, el proveedor conservará únicamente el resultado de la verificación, entendido como los atributos verificados y la referencia que permita individualizar al titular ante requerimiento de autoridad competente, junto con la traza de auditoría del proceso. Las imágenes de documentos de identidad y los datos biométricos utilizados deberán suprimirse de manera definitiva una vez concluida la verificación.

Para efectos de este artículo, la traza de auditoría se limitará a los metadatos estrictamente necesarios para acreditar que la verificación se realizó, tales como la fecha, el mecanismo utilizado y el resultado de la verificación, y en ningún caso podrá contener las imágenes de documentos de identidad, datos biométricos u otra información que permita reconstruir los soportes documentales suprimidos conforme al inciso anterior.

La información relacionada con el resultado de la verificación y la traza de auditoría se almacenará de forma separada de la información pública del perfil, bajo estándares de cifrado y de seguridad de la información, por un término que no podrá exceder doce (12) meses contados desde la desactivación de la respectiva cuenta, salvo que exista un requerimiento vigente de autoridad competente, caso en el cual se conservará hasta su resolución.

Artículo 12. Prohibición de uso comercial. Los datos recolectados para efectos de la verificación de identidad no podrán ser utilizados con fines comerciales, publicitarios o de perfilamiento, ni ser transferidos a terceros no autorizados por parte del titular o autoridades competentes, en los casos previstos en la presente ley.

Parágrafo 1°. Lo dispuesto en este artículo no impide que las plataformas digitales utilicen la información de verificación de identidad para el cumplimiento de sus obligaciones legales de gestión de riesgo y prevención del fraude de identidad, incluyendo las que les correspondan frente a la Superintendencia de Sociedades u otra autoridad de inspección, vigilancia y control aplicable.

Parágrafo 2°. Antes de iniciar la verificación, el proveedor informará al usuario sobre las condiciones de uso de la información de sus documentos de identidad (como su finalidad, su plazo de conservación y los terceros a quienes pueda transferirse con su autorización), de conformidad con este artículo y con el artículo 11°. Esta información se presentará de manera expresa y clara, en una notificación separada de los términos y condiciones generales del servicio. La aceptación de esta notificación no podrá exigirse como condición para el inicio de sesión ni para el acceso del usuario a la plataforma.

Título IV. Ámbito de Aplicación Territorial

Artículo 13. Ámbito de aplicación territorial. Las obligaciones previstas en la presente ley serán exigibles a todos los proveedores de redes sociales y plataformas digitales que permitan el acceso o la creación de cuentas por usuarios ubicados en el territorio de la República de Colombia o que dirijan, ofrezcan o presten sus servicios a personas ubicadas en el territorio nacional. Para efectos de la aplicación de la presente ley, los operadores de redes sociales deberán implementar uno o más mecanismos razonables y proporcionales para determinar que una cuenta corresponde a un usuario ubicado en Colombia, tales como la dirección IP, la geolocalización del dispositivo cuando exista autorización del usuario, el país declarado por el usuario, el código telefónico asociado a la cuenta, el documento de identidad utilizado para la verificación u otros mecanismos tecnológicos equivalentes que determine la reglamentación. Cuando se establezca que una cuenta corresponde a un usuario ubicado en Colombia, el operador deberá dar cumplimiento a las obligaciones de verificación de identidad que le sean exigibles respecto de dicha cuenta conforme al esquema gradual previsto en el artículo 8° de la presente ley, sin que ello implique condicionar de manera general el acceso a la plataforma o a sus contenidos, en los términos del Parágrafo 2° del citado artículo.

Título V. Del Acceso de las Autoridades Competentes a la Información de Identidad

Artículo 14. Acceso mediante orden judicial. Los proveedores de redes sociales y plataformas digitales deberán entregar la información de identidad verificada de un usuario a la Fiscalía General de la Nación o a la autoridad judicial competente, cuando dicha información sea indispensable para la investigación de un delito o la protección de

un derecho fundamental, y medie orden judicial previa, en los términos previstos en la Ley 906 de 2004 y demás normas concordantes, sin perjuicio del procedimiento de urgencia previsto en el artículo 15° de la presente ley.

Artículo 15. Procedimiento de urgencia. En los casos en que exista un riesgo grave, inminente y actual para la vida, la integridad personal o la libertad sexual de una persona, en especial de niños, niñas y adolescentes, la Fiscalía General de la Nación, la Policía Nacional o la autoridad competente que atienda en primer lugar la situación de riesgo podrán requerir la información de identidad de manera urgente, sin perjuicio del control judicial posterior de legalidad, en los términos que establezca la reglamentación. La autoridad distinta de la Fiscalía General de la Nación que formule el requerimiento informará de inmediato a esta, para que se surta dicho control.

Artículo 16. Reserva y cadena de custodia. La información de identidad entregada a las autoridades competentes en virtud de la presente ley tendrá carácter reservado y estará sujeta a las reglas de cadena de custodia previstas en el Código de Procedimiento Penal.

Título VI. Régimen Sancionatorio

Artículo 17. Sanciones administrativas. Los proveedores de redes sociales y plataformas digitales que incumplan las obligaciones previstas en la presente ley serán sancionados administrativamente, previa investigación y con garantía del debido proceso, por la Superintendencia de Industria y Comercio o, en los casos previstos en este artículo, por la autoridad sectorial competente. La Superintendencia de Industria y Comercio, en ejercicio de sus funciones de protección de datos personales, vigilará el cumplimiento de las obligaciones relacionadas con el tratamiento, conservación, seguridad y uso de la información de verificación previstas en la presente ley, e impondrá las sanciones previstas en la Ley 1581 de 2012 y demás normas concordantes. El cumplimiento de las demás obligaciones previstas en esta ley, relacionadas con la verificación de identidad, la determinación de la ubicación territorial de los usuarios y las reglas sobre cuentas automatizadas o inauténticas, será vigilado, y su incumplimiento sancionado, por la autoridad de inspección, vigilancia y control que resulte competente conforme al régimen general aplicable a cada proveedor; a falta de autoridad sectorial competente, la vigilancia y la sanción corresponderán a la Superintendencia de Industria y Comercio, que aplicará las sanciones previstas en la Ley 1581 de 2012 y demás normas concordantes, sin perjuicio de las competencias de otras autoridades.

Las sanciones se graduarán conforme a criterios de proporcionalidad, considerando el tamaño y la capacidad económica del proveedor, la reincidencia y la naturaleza, gravedad y efectos de la infracción, en los términos que defina la reglamentación.

Artículo 18. Circunstancia de agravación punitiva. Adiciónese el numeral 9 al artículo 269H de la Ley 599 de 2000 en el siguiente sentido: "Cuando el delito se cometa

mediante el uso de una cuenta o perfil que suministre información engañosa en los procesos de verificación de identidad previstos en la normatividad vigente."

Título VII. Disposiciones Finales

Artículo 19. Reglamentación. El Gobierno Nacional reglamentará la presente ley dentro de los doce (12) meses siguientes a su promulgación, plazo dentro del cual definirá los mecanismos técnicos de verificación de identidad, los umbrales, criterios e indicadores de que trata el artículo 8°, la metodología y el reporte del número de usuarios de que trata el artículo 4°, y demás aspectos necesarios para su aplicación. Los plazos de implementación para los proveedores son los previstos en el parágrafo transitorio del artículo 8°.

Parágrafo 1°. Previo a la expedición de la reglamentación técnica de que trata este artículo, el Gobierno Nacional convocará mesas de consulta técnica con los gremios del sector y demás actores interesados, con el fin de garantizar la viabilidad técnica y la proporcionalidad de los requisitos que se adopten.

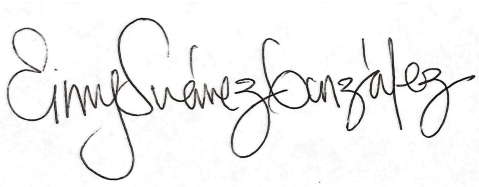
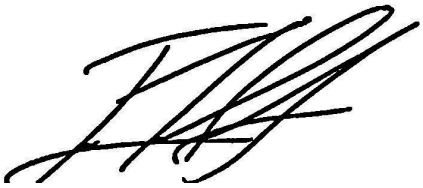
Artículo 20. Vigencia y derogatorias. La presente ley rige a partir de la fecha de su promulgación y deroga todas las disposiciones que le sean contrarias.

Cordialmente,

MIGUEL ÁNGEL PINTO RUEDA
Representante a la Cámara por Santander

Atentamente,

MIGUEL ÁNGEL PINTO RUEDA Representante a la Cámara ***Autor*** Departamento de Santander	**DANIEL BRICEÑO** Representante a la Cámara Bogotá ***Coautor***

 **MAURICIO TORO ORJUELA** Representante a la Cámara Bogotá ***Coautor***	 **Eimy Suárez González** Representante a la Cámara Norte de Santander ***Coautor***
 **JAIME ARIZABALETA FAJARDO** Representante a la Cámara Departamento del Valle del Cauca Partido Centro Democrático	 **JUAN DAVID LONDOÑO ARANGO** Representante a la Cámara Departamento de Vichada Partido de la U
 **MATEO HIDALGO MONTOYA** Representante a la Cámara Caldas ***Coautor***	 **MARTHA ISABEL RUIZ SOLERA** Representante a la Cámara Por Córdoba ***Coautor***

Exposición de Motivos

I. Objeto del proyecto

El presente proyecto de ley estatutaria tiene por objeto:

a) Reconocer y desarrollar el derecho a la identidad digital de las personas, como manifestación de los derechos a la intimidad, al habeas data y al libre desarrollo de la personalidad en entornos digitales.

b) Proteger el anonimato frente al público como elemento del núcleo esencial de la libertad de expresión (Marco Normativo, sección V), sin que ello impida la trazabilidad mínima de los usuarios frente a la autoridad competente, bajo garantías de reserva y control judicial.

c) Establecer un esquema gradual de verificación de identidad, proporcional al riesgo, aplicable a los proveedores de redes sociales y plataformas digitales que operen en Colombia o presten servicios a usuarios ubicados en el país.

d) Fortalecer las herramientas institucionales para la prevención, investigación y sanción de los delitos cometidos a través de entornos digitales, entre ellos la suplantación de identidad, el acoso, la extorsión, el fraude, el grooming, la explotación sexual de niños, niñas y adolescentes, y la manipulación coordinada de la opinión pública mediante cuentas automatizadas o inauténticas.

e) Garantizar que las medidas anteriores se ejerzan bajo los principios de proporcionalidad, minimización, finalidad, reserva, debido proceso y no discriminación (Título I), sin afectar el ejercicio legítimo de la libertad de expresión.

II. Justificación y conveniencia del proyecto

1. El problema que atiende el proyecto. Tres fenómenos, documentados con cifras oficiales recientes, justifican la intervención legislativa.

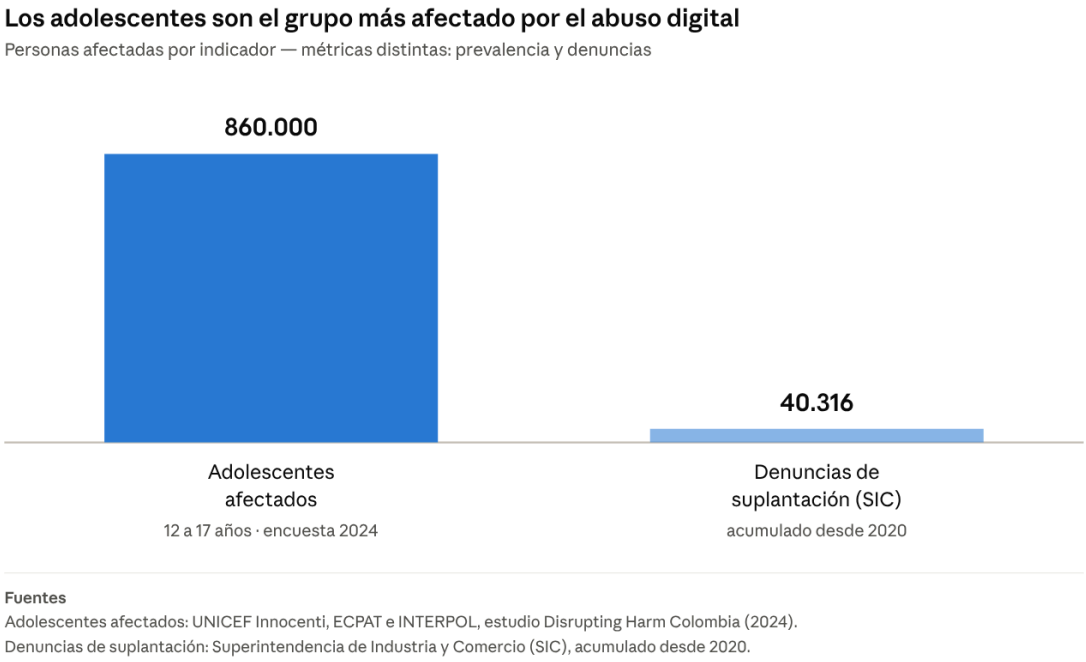
En suplantación de identidad y fraude digital, la Superintendencia de Industria y Comercio[1] ha recibido 40.316 denuncias por suplantación de identidad desde 2020 ante su Delegatura de Protección de Datos Personales —13.983 de ellas desde 2022 a través de SIC Facilita, el 81% relacionadas con telecomunicaciones— y ha impuesto multas por más de $2.390 millones a operadores por fallas de verificación. En el mismo sentido, el boletín de seguimiento de la Policía Nacional[2] registró 44.773 delitos informáticos en el primer semestre de 2026 —un aumento del 35% frente al mismo período de 2025 (33.057

[1] Superintendencia de Industria y Comercio, alerta por aumento de suplantación de identidad. Disponible en: https://sedeelectronica.sic.gov.co/noticias/la-sic-alerta-por-aumento-de-suplantacion-de-identidad-en-el-pais-y-lanza-campana-para-prevenir-fraudes-digitales

[2] El Nuevo Siglo, con base en el boletín de seguimiento de la Policía Nacional, delitos informáticos aumentaron un 35% en el primer semestre de 2026. Disponible en: https://www.elnuevosiglo.com.co/nacion/delitos-informaticos-aumentaron-un-35-en-el-primer-semestre-de-2026

casos) y la cifra semestral más alta de la última década—, con la suplantación y la clonación de cuentas entre las modalidades más frecuentes.

En explotación sexual y grooming de niños, niñas y adolescentes, el estudio Disrupting Harm Colombia[3] de UNICEF Innocenti, ECPAT International e INTERPOL —publicado el 6 de mayo de 2026, con base en una encuesta realizada en 2024 a 999 adolescentes de 12 a 17 años, en el marco de una investigación desarrollada entre 2023 y 2025— encontró que uno de cada cinco adolescentes usuarios de internet en Colombia (21%, cerca de 860.000 niñas, niños y adolescentes entre 12 y 17 años) sufrió alguna forma de abuso o explotación sexual facilitada por la tecnología en un solo año, un fenómeno que describe como "uno de los principales escenarios" para estos delitos; entre esas conductas se reportan el envío de imágenes sexuales no deseadas (15%), ofertas de dinero o regalos a cambio de contenido sexual (6%) y presión o chantaje para no compartir material sexual (5%) — patrones característicos de grooming y sextorsión que dependen, en buena parte, de la facilidad para operar cuentas no verificadas frente a menores.



Un caso reciente, fallado en noviembre de 2025 por un juzgado de Medellín[4], ilustra ese patrón: un hombre que se hizo pasar por una mujer en redes sociales y que ganó durante

[3] UNICEF Innocenti, ECPAT International e INTERPOL, Disrupting Harm Colombia, comunicado de prensa, 6 de mayo de 2026. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/en-un-solo-a%C3%B1o-1-de-cada-5-adolescentes-en-colombia-sufri%C3%B3-abusos-y-explotaci%C3%B3n

[4] Vanguardia, caso fallado en noviembre de 2025 por un juzgado de Medellín. Disponible en: https://www.vanguardia.com/colombia/2025/11/21/se-hizo-pasar-por-mujer-para-abusar-de-una-nina-pagara-14-anos-de-carcel/

varias semanas la confianza de una menor de edad, obtuvo de ella imágenes íntimas y luego la extorsionó —exigiéndole dinero y, bajo amenaza de difundirlas, acceso sexual—, delito por el cual fue condenado a 14 años de prisión, condena de primera instancia actualmente en apelación ante el Tribunal Superior de Medellín. Ese patrón —contacto bajo identidad falsa, generación de confianza y extorsión posterior— es el que la Policía Nacional identifica de forma recurrente en sus alertas sobre depredadores digitales[5], y es exactamente el que una verificación mínima frente a la autoridad, sin exposición pública de la identidad, permitiría hacer trazable.

En manipulación coordinada mediante cuentas automatizadas o inauténticas, organizaciones de observación electoral y medios especializados han documentado de forma recurrente la operación de redes de cuentas falsas y bots en el debate público colombiano, en particular alrededor de procesos electorales, generando preocupación institucional sobre la integridad de la información que circula en plataformas digitales.

Los tres fenómenos comparten una causa estructural que el ordenamiento vigente no cierra: ningún proveedor de redes sociales o plataformas digitales está hoy obligado, de forma general, a verificar, así sea de forma mínima, que detrás de una cuenta hay una persona real e identificable ante la autoridad competente. Las normas más cercanas son parciales: la Ley 2489 de 2025 y el Decreto 769 de 2026 establecen la verificación de edad en los entornos digitales de niños, niñas y adolescentes, y la Ley Estatutaria 2573 de 2026 adopta medidas frente a la suplantación de identidad en telecomunicaciones, entidades financieras y establecimientos de comercio (Marco Normativo, sección V.B). El proyecto no busca eliminar el anonimato frente al público —que la jurisprudencia constitucional protege como elemento del núcleo de la libertad de expresión (Marco Normativo, sección V)—, sino cerrar esa brecha únicamente frente a las autoridades, bajo garantías de reserva, minimización y control judicial.

A esos tres fenómenos se suma uno cuya regulación la Corte Constitucional ha reiterado al Congreso: la violencia de género digital. En la Sentencia T-348 de 2026 (27 de octubre de 2026), la Corte amparó a la gestora social del municipio de Arauca, a quien un creador de contenido atacó en Facebook con publicaciones sobre su cuerpo, supuestas cirugías estéticas y su vida familiar. Concluyó que los discursos que constituyen violencia de género contra las mujeres no están protegidos por la libertad de expresión; que la crítica a la gestión pública sí lo está, pero no el desplazamiento del debate hacia el cuerpo o la apariencia de una mujer; y que los medios digitales pueden constituir espacios hostiles para ellas, con efectos de autocensura y de silenciamiento de su participación. Advirtió, además, que los agresores pueden ejercer esa violencia desde el anonimato, y reiteró el exhorto formulado en las Sentencias T-280 de 2022, T-087 de 2023 y SU-432 de 2025 para que el Congreso atienda las recomendaciones formuladas por el Consejo de

[5] El Tiempo, así depredadores digitales captan a menores en redes y videojuegos, con base en alertas de la Policía Nacional. Disponible en: https://www.eltiempo.com/justicia/delitos/asi-depredadores-digitales-captan-a-menores-en-redes-y-videojuegos-para-obtener-imagenes-intimas-esta-es-la-alerta-de-la-policia-3551181

Derechos Humanos de las Naciones Unidas y por la Organización de los Estados Americanos sobre prevención, protección, reparación, prohibición y penalización de la violencia de género digital.

Este proyecto no pretende tipificar ni regular de forma específica esa violencia, que requiere una regulación propia. Aporta, en cambio, una herramienta que cualquier respuesta seria necesita: que la autoridad judicial pueda identificar al autor de una agresión cuando actúa tras un perfil anónimo o inauténtico, bajo orden judicial previa o, en urgencia, con control judicial posterior, y sin que su identidad se exponga al público (arts. 6°, 7°, 14° y 15°).

2. Por qué la respuesta es proporcionada. El proyecto no impone una verificación de identidad universal, indiscriminada ni pública. Sigue un esquema gradual por nivel de riesgo (art. 8°): verificación previa obligatoria solo para quienes monetizan, pautan publicidad, alcanzan audiencias masivas mediante promoción del proveedor o administran cuentas de menores; verificación reactiva ante indicios objetivos de suplantación, operación automatizada o comisión de delitos; y, para el resto de las cuentas, un atributo mínimo verificado que nunca se hace público y que solo se entrega a la autoridad competente mediante orden judicial previa (Título V). Esa identidad verificada pero no divulgada es lo que permite conciliar la protección del anonimato frente al público (arts. 5° a 7°) con la trazabilidad mínima frente a la autoridad que el proyecto busca garantizar.

3. Por qué esta versión del proyecto es el punto de equilibrio correcto. El articulado que se radica no es la primera versión discutida. Antes de esta radicación se consultó a cuatro gremios con intereses y posiciones distintas: Alianza IN (cuya propuesta constituye la base aprobada del articulado), la Cámara Colombiana de Comercio Electrónico (CCCE), FEDESOFT y la Asociación Latinoamericana de Internet (ALAI). El proceso de conciliación de esas cuatro posiciones —documentado en detalle en la Tabla de Cambios Unificados – PL Identidad Digital— incorporó al articulado los ajustes técnicamente compatibles con su objeto: acotamiento del ámbito de aplicación a servicios de interacción pública (CCCE); equivalencia con regímenes de debida diligencia ya existentes y una cláusula de diligencia debida para proveedores de buena fe (FEDESOFT); alternativas de verificación mediante prestadores de confianza digital acreditados y un mecanismo alternativo no biométrico siempre disponible (FEDESOFT y ALAI); y graduación de las sanciones por tamaño del proveedor (FEDESOFT), entre otros.

El proyecto también decidió, de forma deliberada y razonada, no acoger dos objeciones de fondo planteadas por ALAI: la eliminación de toda exigencia mínima de verificación, y la eliminación del alcance extraterritorial de la ley. La primera vaciaría el objeto central del proyecto —la trazabilidad mínima frente a autoridades—. La segunda, además de dejar sin protección a los usuarios colombianos frente a plataformas extranjeras, se apoya en una lectura de la jurisprudencia de la Corte Constitucional que, leída en su texto completo, respalda exactamente lo contrario (Sentencias C-527 de 2003 y T-1157 de 2000; Marco Normativo, sección V).

La Corte Constitucional ha explicado esa regla en estos términos literales: en la Sentencia C-527 de 2003, los actos iniciados en el exterior son alcanzables por la ley colombiana cuando "culminaron o tienen efectos sustanciales y directos dentro de él [el territorio nacional]"; en la Sentencia T-1157 de 2000, de forma equivalente, cuando "se ejecutan o tienen efectos dentro de sus fronteras territoriales". Las plataformas extranjeras que prestan servicios a usuarios ubicados en Colombia se ajustan exactamente a ese supuesto.

4. Experiencia internacional comparada y urgencia de la intervención. Colombia no sería el primer país en legislar sobre esta materia; varias jurisdicciones comparables ya exigen algún mecanismo de verificación de edad o identidad en plataformas digitales. Australia[6] reformó su Online Safety Act 2021 (Parte 4A) para prohibir, desde el 10 de diciembre de 2025, que las plataformas de redes sociales permitan cuentas de menores de 16 años; de forma relevante para el diseño de este proyecto, esa ley impide exigir un servicio de identidad digital acreditado como único mecanismo de verificación, dejándolo como una opción entre varias. El Reino Unido[7], bajo la Online Safety Act 2023, exige a las plataformas un estándar de verificación de edad "altamente efectivo" —supervisado por Ofcom, con sanciones de hasta 18 millones de libras o el 10% de la facturación global, lo que sea mayor— que descarta expresamente mecanismos débiles como una casilla de verificación o una fecha de nacimiento autodeclarada. La Unión Europea, a través del Reglamento eIDAS 2.0, construyó precisamente la figura que FEDESOFT propuso para este proyecto (Tabla de Cambios Unificados, art. 9°): prestadores de servicios de confianza digital acreditados e interoperables, como alternativa a depender de un único verificador estatal.

La urgencia de la intervención no es solo comparada. Los delitos informáticos registrados en Colombia crecieron 35% en un semestre frente al mismo período del año anterior —la cifra semestral más alta de la última década (sección II.1)—, mientras el país sigue sin un mecanismo mínimo de verificación frente a la autoridad. Cada período de demora en la radicación y el trámite de este proyecto es, en los términos de esa misma estadística, un período adicional de crecimiento del fenómeno sin respuesta institucional.

III. Contenido del proyecto

El articulado —Borrador Articulado Consolidado – PL Identidad Digital (Alianza IN + CCCE)— se organiza en siete títulos:

- **Título I. Disposiciones generales** (arts. 1° a 4°): objeto, ámbito de aplicación, principios (proporcionalidad, minimización, finalidad, reserva, debido proceso, no discriminación) y definiciones.

[6] Gobierno de Australia, Online Safety Act 2021 (Parte 4A) y sistema de verificación de edad. Disponible en: https://www.digitalidsystem.gov.au/news/social-media-minimum-age-verification-law-and-digital-id

[7] AU10TIX, Online Safety Act 2023 del Reino Unido. Disponible en: https://www.au10tix.com/blog/uk-online-safety-act/

- **Título II. Del derecho a la identidad digital y del anonimato frente al público** (arts. 5° a 7°): reconoce el derecho a la identidad digital, protege el anonimato frente al público y limita su divulgación a supuestos excepcionales.
- **Título III. De la verificación de identidad en plataformas digitales** (arts. 8° a 12°): fija el esquema gradual de verificación por nivel de riesgo, los mecanismos admitidos, las reglas de verificación de menores, y los límites a la conservación y uso de la información recolectada.
- **Título IV. Ámbito de aplicación territorial** (art. 13°): extiende las obligaciones a proveedores extranjeros que presten servicios a usuarios ubicados en Colombia.
- **Título V. Del acceso de las autoridades competentes a la información de identidad** (arts. 14° a 16°): condiciona la entrega de información a orden judicial previa, salvo procedimiento de urgencia con control judicial posterior.
- **Título VI. Régimen sancionatorio** (arts. 17° y 18°): distribuye la vigilancia entre la Superintendencia de Industria y Comercio y las autoridades sectoriales competentes, y adiciona una circunstancia de agravación punitiva (art. 269H de la Ley 599 de 2000) para los delitos informáticos cometidos mediante una cuenta o perfil que suministre información engañosa en la verificación de identidad.
- **Título VII. Disposiciones finales** (arts. 19° y 20°): reglamentación, vigencia y derogatorias.

IV. Antecedentes — proceso de consulta con los gremios

El articulado que se radica es el resultado de un proceso de consulta secuencial con los actores del sector:

1. Alianza IN presentó una propuesta base de articulado, revisada y aprobada como punto de partida del proyecto.
2. La Cámara Colombiana de Comercio Electrónico (CCCE) remitió observaciones sobre la amplitud del ámbito de aplicación, la vaguedad de algunos umbrales del art. 8°, la indefinición de la "traza de auditoría" del art. 11°, y la posible afectación de la reserva de ley estatutaria, entre otras.
3. FEDESOFT remitió observaciones técnicas adicionales, en un tono mayoritariamente favorable al proyecto, centradas en evitar duplicidad regulatoria, ampliar las alternativas técnicas de verificación, y graduar las sanciones.
4. ALAI remitió observaciones de carácter más estructural, cuestionando el alcance extraterritorial del proyecto, la existencia misma de un esquema de verificación mínima, y la idoneidad de la infraestructura de la Registraduría Nacional del Estado Civil, entre otras.

Cada observación fue evaluada frente al objeto del proyecto; la Tabla de Cambios Unificados – PL Identidad Digital documenta, artículo por artículo, qué se incorporó, qué se decidió no acoger y por qué. Se reproduce a continuación en su integridad.

Art.	Cambio incorporado (Alianza IN, aprobado)	Observaciones de los gremios	Estado	Nota
4 (definiciones)	"Plataformas digitales" se acota a "plataformas de redes sociales" en la definición de anonimato; se agrega la salvedad "no autorizados por el titular"; en "cuenta inauténtica" cambia "o" por "y/o" (técnico).	CCCE y FEDESOFT piden lo mismo: distinguir tipos de plataforma según el riesgo del modelo de negocio (mensajería, marketplaces, B2B, educativas, videojuegos).	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado (art. 2°) acota el ámbito a plataformas de interacción pública y excluye expresamente mensajería, marketplaces, B2B, productividad, videojuegos sin función social y comunidades privadas — responde a las dos observaciones.
6 (anonimato frente al público)	Se elimina "y plataformas digitales"; el uso de seudónimos queda garantizado solo dentro de redes sociales.	CCCE: "no podrá ser restringido por los proveedores" puede chocar con deberes de identificación en comercio electrónico (Ley 1480 de 2011, art. 50).	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado agrega una frase final reconociendo esos otros deberes legales.
8 (obligación de verificación)	Reescritura total: esquema gradual de 3 niveles (previa obligatoria / por riesgo / régimen general), con parágrafos y plazos transitorios de 12 y 24 meses.	CCCE: literal 1.c (umbrales sin criterio claro) y "régimen general" universal. FEDESOFT: la verificación por monetización (num. 1.a) se solapa con el KYC que ya exige el régimen SARLAFT/UIAF a entidades vigiladas. ALAI: sostiene que todo el esquema —incluido el régimen general— anula el anonimato frente al proveedor (no solo frente al público), que el literal 1.c opera como censura previa (art. 20 C.P.), que el numeral 2 delega una función de juzgamiento a las plataformas sin orden judicial, y que el numeral 3 equivale a perfilamiento	Parcialmente incorporado / objeción de fondo de ALAI no acogida	El borrador consolidado precisa los umbrales (parágrafo 3°) y agrega criterios diferenciados para los proveedores que no sean de gran escala (responde a CCCE). También define al proveedor de gran escala (art. 4°) y gradúa los plazos del parágrafo transitorio: 12 meses (numeral 1) y 24 meses (numerales 2 y 3) para esos proveedores, y 12 meses adicionales para los demás. Incorpora la exención KYC de FEDESOFT (parágrafo 4°) y acota el literal 1.c a la difusión amplificada por el proveedor (no alcance orgánico). La objeción de ALAI es un

Art.	Cambio incorporado (Alianza IN, aprobado)	Observaciones de los gremios	Estado	Nota
		continuo de toda la base de usuarios.		desacuerdo de fondo sobre si cualquier verificación mínima es constitucional: no se acoge, porque desmontaría el objetivo central del proyecto; SU-420/2019 protege el anonimato frente al público, no necesariamente frente al intermediario.
9 (mecanismos / prueba de vida)	Verificación por atestación de atributos sin que el proveedor reciba o almacene el documento ni datos biométricos; prueba de vida condicionada a recursos tecnológicos/ financieros de la plataforma; nuevo parágrafo de equivalencia con la Ley Estatutaria 2573 de 2026.	CCCE: la prueba de vida debería depender del riesgo, no del tamaño del proveedor. FEDESOFT: la infraestructura de la Registraduría no tiene SLA ni capacidad de escalamiento conocidos; propone crear "prestadores de servicios de confianza digital" acreditados (análogos a eIDAS 2.0), interoperables con estándares abiertos. ALAI: coincide en el riesgo de saturación de la Registraduría; añade que la prueba de vida biométrica tiene tasas de falso rechazo más altas en personas mayores, con discapacidad o cierto tono de piel, y excluye a quienes no tienen cámaras de alta resolución o banda ancha.	Incorporado	El borrador consolidado liga la prueba de vida al riesgo (responde a CCCE), con lo que elimina la condición de recursos de la plataforma: la define la reglamentación, sin que el proveedor reciba ni almacene datos biométricos. Incorpora la figura de "prestadores de servicios de confianza digital" que propuso FEDESOFT y exige siempre un mecanismo alternativo no biométrico, como pidió ALAI.
10 (cuentas de menores)	La verificación plena de quien ejerce patria potestad/custodia/ representación legal se reemplaza por una declaración jurada de "un adulto responsable".	CCCE: la representación legal no siempre se puede demostrar con una simple declaración; pide graduar por riesgo. FEDESOFT: verificar la representación legal sin acceso a registros de filiación es poco viable; pide reconocer mecanismos de verificación parental y age	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado gradúa la doble verificación por riesgo (Ley 2489/2025 y Decreto 769/2026), que es en sustancia lo que piden los tres, y reconoce los mecanismos de verificación parental y de estimación de edad

Art.	Cambio incorporado (Alianza IN, aprobado)	Observaciones de los gremios	Estado	Nota
		assurance ya validados internacionalmente. ALAI: la doble verificación universal choca con la autonomía progresiva de NNA (cita Sentencia T-391 de 2007) y puede empujarlos a plataformas sin ninguna protección.		con validación técnica internacional que pide FEDESOFT.
11 (conservación de datos)	Solo se conserva el resultado de verificación + "traza de auditoría"; supresión definitiva obligatoria de imágenes de documentos y biometría al concluir la verificación; tope de 12 meses desde la desactivación de la cuenta.	CCCE: "traza de auditoría" no está definida y podría reconstruir información personal significativa. ALAI: conservar la vinculación identidad–cuenta hasta 12 meses crea un repositorio centralizado, blanco de ciberataques; pide un plazo más corto o ninguno sin investigación en curso.	Incorporado en el Borrador Articulado Consolidado (parcial)	El borrador consolidado define "traza de auditoría" como metadatos mínimos, sin documentos ni biometría (responde a CCCE). Acortar el plazo de 12 meses que pide ALAI es una decisión de alcance, no de redacción.
12 (prohibición de uso comercial)	"Terceros distintos de las autoridades competentes" pasa a "terceros no autorizados por el titular o autoridades competentes"; nuevo parágrafo que permite usar la información para gestión de riesgo/prevención de fraude frente a la Superintendencia de Sociedades u otra autoridad IVC.	Sin observaciones de CCCE, FEDESOFT ni ALAI.	Sin observaciones	Cambio propio de Alianza IN.
13 (ámbito territorial)	Exige "una combinación de mecanismos	CCCE: combinar señales incentiva recolectar más datos de los necesarios.	Tensión directa (Alianza IN vs.	El borrador consolidado suaviza a "uno o más mecanismos

Art.	Cambio incorporado (Alianza IN, aprobado)	Observaciones de los gremios	Estado	Nota
	razonables" (antes solo "mecanismos razonables") para determinar la ubicación del usuario en Colombia.	FEDESOFT: el costo de cumplir recae más sobre startups/pymes colombianas que sobre plataformas globales. ALAI: cuestiona la extraterritorialidad misma (cita Sentencia C-527 de 2003 y T-1157 de 2000) y los mecanismos del artículo (IP, geolocalización) por intrusivos y poco fiables (VPN, roaming).	CCCE) + objeción de fondo de ALAI no acogida	razonables y proporcionales". Sobre la extraterritorialidad: las mismas sentencias que cita ALAI, leídas completas, reconocen que Colombia puede aplicar su ley a hechos con "efectos sustanciales y directos" en el país. No se acoge remover el alcance extraterritorial.
17 (régimen sancionatorio)	Sin cambios de Alianza IN frente al texto radicado.	CCCE: la competencia de la SIC ("en ejercicio de sus funciones de protección de datos") no cubre obligaciones que van más allá del tratamiento de datos. FEDESOFT: pide criterios expresos de proporcionalidad y gradualidad sancionatoria según tamaño de empresa, reincidencia y naturaleza de la infracción.	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado acota la competencia de la SIC a lo propiamente de datos y remite el resto a la autoridad sectorial (responde a CCCE), y gradúa las sanciones considerando también el tamaño y la capacidad económica del proveedor, atendiendo la solicitud de FEDESOFT.
18 (agravante penal)	El hecho agravante pasa de "cuenta que incumpla la obligación de verificación" a "cuenta que suministre información engañosa en los procesos de verificación".	Sin observaciones de CCCE, FEDESOFT ni ALAI.	Sin observaciones	Mejora técnica propia de Alianza IN.
19 (reglamentación)	Sin cambios de Alianza IN frente al texto radicado.	FEDESOFT: pide un mandato expreso de mesas técnicas de consulta con los gremios del sector antes de expedir la reglamentación, con plazos definidos.	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado agrega un parágrafo que ordena al Gobierno convocar mesas de consulta técnica con los gremios del sector y demás actores interesados antes de

Art.	Cambio incorporado (Alianza IN, aprobado)	Observaciones de los gremios	Estado	Nota
				expedir la reglamentación técnica, y fija los plazos: doce meses para reglamentar (art. 19°) y los de implementación del parágrafo transitorio del art. 8°.
General (responsabilidad)	No existe un artículo dedicado a esto en ninguna versión.	FEDESOFT: pide una cláusula de "diligencia debida" (safe harbor) que exonere al proveedor cuando haya implementado razonablemente los mecanismos exigidos y el usuario burle el sistema con documentos falsificados.	Incorporado en el Borrador Articulado Consolidado	El borrador consolidado agrega el parágrafo 5° del art. 8°: el proveedor que haya implementado razonablemente los mecanismos de verificación exigidos por la ley y su reglamentación no es responsable cuando un usuario los eluda con documentos o atributos falsificados, sin perjuicio de la responsabilidad del autor de la falsificación.

Artículos 1, 3, 5, 7, 14, 15, 16 y 20: sin cambios entre el texto radicado y la versión de Alianza IN. El artículo 2 tampoco cambió frente al texto radicado, pero las observaciones de ámbito de aplicación de CCCE, FEDESOFT y ALAI que lo mencionan junto con el art. 4 se resumen en la fila "4 (definiciones)".

Ajustes posteriores a la consulta. Además de lo recogido en la tabla, en la versión final del proyecto el proponente introdujo, por iniciativa propia, los siguientes ajustes:

- Personas jurídicas (arts. 2°, 4° y 8°, parágrafo 6°): el ámbito de aplicación, la definición de verificación de identidad y un nuevo parágrafo incluyen a las personas jurídicas titulares de cuentas, cuya verificación comprende también a su representante legal.
- Art. 6°: se denomina «Anonimato frente al público» y se precisa que no es absoluto y que las autoridades competentes pueden limitarlo, de conformidad con la Constitución y la ley.
- Art. 7° (parágrafo 1° y causal iii): la información privada del usuario solo se entrega al titular o a las autoridades facultadas, dentro de lo estrictamente necesario, y no puede compartirse con otros terceros; la causal (iii) incluye a las autoridades del procedimiento de urgencia del art. 15°.

- Art. 9° (nuevo inciso): mecanismo interno de apelación del resultado de la verificación y canal de comunicación accesible para atender caídas, fallas o errores, atendidos por una persona natural.
- Art. 12° (parágrafo 2°): el proveedor informa las condiciones de uso de la información de los documentos en una notificación separada, cuya aceptación no puede condicionar el acceso del usuario a la plataforma.
- Art. 15°: el procedimiento de urgencia se extiende a la Policía Nacional y a la autoridad competente que atienda en primer lugar la situación de riesgo, con aviso inmediato a la Fiscalía General de la Nación para el control judicial posterior.
- Art. 17°: se establece expresamente que el incumplimiento de las obligaciones de la ley es sancionado por la Superintendencia de Industria y Comercio o, en los casos previstos, por la autoridad sectorial competente.

V. Marco normativo

Como el proyecto va a tramitarse como ley estatutaria por Comisión Primera, este marco normativo reúne las sentencias y normas citadas en las retroalimentaciones de los gremios (principalmente en las cartas de CCCE, FEDESOFT y ALAI) y en el análisis previo de este proyecto, explicando qué respalda cada una dentro del articulado. Las sentencias fueron verificadas contra las páginas de relatoría oficiales de la Corte Constitucional.

A. Jurisprudencia constitucional

Sentencia C-413 de 2025. Revisó el proyecto de ley estatutaria que se convirtió en la Ley Estatutaria 2573 de 2026, sobre protección de personas víctimas de suplantación de identidad en telecomunicaciones y el sector financiero. La Corte concluyó que debía tramitarse como ley estatutaria por un criterio formal (modificaba una ley ya estatutaria) y uno material (regula el núcleo del habeas data: principios, reglas, definiciones, derechos y deberes sobre administración de datos personales). Definió la suplantación de identidad como el uso no consentido de información personal de otro, generalmente con fines fraudulentos, y validó medidas como la suspensión inmediata de cobros al reportarse la suplantación, la corrección de reportes negativos y la inversión de la carga de la prueba en sede administrativa. *Qué respalda:* es el precedente directo para tramitar este proyecto como ley estatutaria, y aporta una definición de "suplantación de identidad" y ejemplos de medidas protectoras que sirven de referente para el Título III y el régimen sancionatorio.

Sentencia SU-420 de 2019. Estableció que el anonimato es "un elemento esencial del derecho a la libertad de expresión" en internet, y que la posibilidad de publicar contenido de forma anónima —incluso mediante herramientas de cifrado— está protegida constitucionalmente. Precisó que esa protección no es absoluta: cede frente a publicaciones sin un fin constitucional legítimo o con la única intención de dañar que no

aporten al debate público. Asimismo, fijó cargas procesales estrictas para las tutelas entre particulares (solicitud de retiro al autor, reclamo formal a la plataforma y un análisis ponderado de quién comunica, sobre quién y cómo). *Qué respalda:* Funciona como el fundamento constitucional directo del anonimato en el ecosistema digital, entendido como elemento de la libertad de expresión, y confirma que admite límites y responsabilidades ulteriores. Esto legitima constitucionalmente el esquema de "verificación silenciosa" (donde la identidad es conocida o verificable por el sistema para responder ante eventuales abusos, pero se mantiene reservada frente al público para proteger la libertad de expresión).

Sentencia T-275 de 2021. Analizó el "escrache" o la denuncia pública digital de conductas delictivas o de violencia basada en género en redes sociales, en tensión con la honra, el buen nombre y la presunción de inocencia del denunciado. La Corte reconoció que el escrache goza de una protección constitucional reforzada como herramienta de control social ante la ineficacia del sistema judicial ordinario. No obstante, aclaró que esta protección no es absoluta: exige el cumplimiento de un estándar flexible pero responsable de veracidad e imparcialidad, prohibiendo el insulto puro, la difamación evidente o la revelación de datos médicos sensibles sin justificación. *Qué respalda:* Valida el derecho de las víctimas y la ciudadanía a realizar denuncias públicas en entornos virtuales sin necesidad de esperar un fallo judicial previo. Al articularse con las reglas generales de internet, confirma que la responsabilidad por los excesos del discurso recae exclusivamente sobre quien emite la información, protegiendo las dinámicas de visibilización comunitaria e institucional siempre que respeten las garantías procesales mínimas (arts. 7°, 14° y 15°).

Sentencias C-729 de 2000 y C-1011 de 2008. Constituyen la piedra angular de la doctrina constitucional del derecho al habeas data (art. 15 C.P.) en Colombia. La Sentencia C-729 de 2000 fijó la regla de reserva de ley estatutaria, determinando que cualquier regulación integral, límite o condición de ejercicio de los derechos fundamentales a la información y protección de datos personales está vedada para el legislador ordinario. Por su parte, la Sentencia C-1011 de 2008 realizó el control previo de constitucionalidad del proyecto que se convirtió en la Ley 1266 de 2008 (habeas data financiero), definiendo la tipología de los datos (públicos, privados, semiprivados y reservados) y fijando el límite de caducidad del dato negativo (máximo 4 años tras el pago), lo que impide las sanciones comerciales perpetuas. *Qué respalda:* establece el bloque de legalidad y el debido proceso para la administración de bases de datos, y sustenta que la información financiera y de comportamiento comercial es un dato semiprivado cuyo tratamiento legítimo exige consentimiento, notificación previa y un término de permanencia proporcional — precisamente la base doctrinal que sostiene la decisión de tramitar este proyecto como ley estatutaria.

Sentencia T-241 de 2023. Estudió la tensión entre el derecho al buen nombre de un ciudadano y la libertad de expresión de una mujer que, utilizando un perfil anónimo en

Facebook, realizó un "escrache" o denuncia pública acusándolo de violencia sexual, física y psicológica. La Corte determinó que el escrache feminista digital es una manifestación protegida constitucionalmente y una respuesta legítima ante las deficiencias institucionales y la violencia de género. El fallo dispuso que, en contextos de agresiones contra la mujer, la preservación del anonimato de la denunciante goza de protección reforzada para salvaguardar su seguridad y evitar su revictimización. Por consiguiente, negó la retractación solicitada por el accionante. *Qué respalda:* consolida el fundamento constitucional que justifica la confluencia entre el anonimato frente al público y el enfoque de género (arts. 7°, 14° y 15°). Sustenta que las denuncias anónimas sobre violencia de género no pueden ser censuradas ni forzadas a una retractación automática bajo el mero alegato de la presunción de inocencia, y refuerza que las herramientas de verificación de identidad no deben quebrantar la reserva del perfil ante el debate público, para no desincentivar la denuncia comunitaria.

Sentencia T-348 de 2026. Resolvió la tutela de la gestora social del municipio de Arauca contra un creador de contenido que publicó en Facebook material sobre su cuerpo, supuestas cirugías estéticas y su vida familiar. La Corte revocó el fallo que negaba el amparo y concluyó que los discursos que constituyen violencia de género contra las mujeres no están protegidos por la libertad de expresión. Separó la crítica a la gestión pública, que sigue amparada, de las expresiones sobre el cuerpo, la apariencia o la intimidad de la mujer, y fijó tres preguntas para el juez: si el contenido recurre a estereotipos de género, sexualización o cosificación; si hay un patrón reiterado de hostigamiento o descrédito; y si puede producir un efecto inhibidor o silenciador sobre su participación en el espacio público. Ordenó al autor retirar las publicaciones, abstenerse de repetirlas, ofrecer una disculpa pública y capacitarse en igualdad de género, y reiteró al Congreso el exhorto de las Sentencias T-280 de 2022, T-087 de 2023 y SU-432 de 2025 sobre prevención, protección, reparación, prohibición y penalización de la violencia de género digital. *Qué respalda:* no trata la verificación de identidad —el autor actuaba con su propio nombre—, pero advierte que los agresores pueden ejercer esa violencia desde el anonimato y confirma que la libertad de expresión, como el anonimato (SU-420 de 2019), no es absoluta. Leída con la T-241 de 2023, que protege el anonimato de la mujer que denuncia, ilustra el equilibrio del proyecto: reserva de la identidad frente al público (arts. 6° y 7°) y acceso de la autoridad a ella bajo control judicial (arts. 14° y 15°). El proyecto no pretende tipificar esa violencia ni atender por sí solo el exhorto, que requiere una regulación específica.

Sentencia C-336 de 2007. Declaró la exequibilidad condicionada de los artículos 14 y 244 de la Ley 906 de 2004 (Código de Procedimiento Penal). La Corte determinó que la búsqueda selectiva en bases de datos computarizadas o mecánicas que no sean de libre acceso (información confidencial, sensible o reservada de un indiciado o imputado) afecta directamente el derecho fundamental a la intimidad. En consecuencia, estableció que la Fiscalía no puede ordenar autónomamente estas búsquedas; por el contrario, requiere obligatoriamente una autorización judicial previa del juez de control de garantías, seguida

de una audiencia de control posterior dentro de las treinta y seis (36) horas siguientes para examinar su legalidad formal y material. *Qué respalda:* es el fundamento directo del ajuste ya incorporado al art. 14° del proyecto —que exige orden judicial previa y elimina la alternativa de "requerimiento formal" de la Fiscalía—, y responde tanto a la observación original de CCCE como a la que formula ALAI sobre reserva judicial.

Sentencia T-391 de 2007. Sobre contenido sexualmente explícito difundido por radio: protegió la libertad de expresión del medio, pero confirmó que es constitucionalmente válido imponer límites razonables y proporcionados cuando el público incluye niños, niñas y adolescentes, sin que ello equivalga a censura previa. *Qué respalda:* ALAI la invoca a propósito de la doble verificación de menores del art. 10°. La sentencia respalda, en realidad, el criterio que ya sigue ese artículo: protección reforzada de menores mediante límites proporcionados y graduados, no mediante una regla absoluta o indiferenciada.

Sentencias C-527 de 2003 y T-1157 de 2000. Desarrollan el principio de "territorialidad objetiva": la Corte reconoce que el Estado colombiano puede aplicar sus normas a actos iniciados en el exterior cuando culminan o producen efectos sustanciales y directos dentro del territorio nacional (C-527 de 2003, sobre tributación de servicios técnicos prestados desde el exterior; T-1157 de 2000, sobre bienes y contratos con elementos extranjeros vinculados a Colombia). *Qué respalda:* ALAI invoca ambas sentencias para cuestionar el alcance extraterritorial del art. 13°. Leídas en su texto completo, respaldan lo contrario: las plataformas extranjeras que prestan servicios a usuarios ubicados en Colombia producen exactamente los efectos sustanciales y directos que, según esta misma jurisprudencia, habilitan la aplicación de la ley colombiana. Por esta razón el proyecto mantiene el alcance extraterritorial del artículo.

B. Marco legal y reglamentario

- **Constitución Política, arts. 15, 20, 44 y 152 lit. a):** habeas data e intimidad; libertad de expresión; derechos de los niños, niñas y adolescentes; reserva de ley estatutaria.
- **Ley Estatutaria 1581 de 2012:** régimen general de protección de datos personales (finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad, confidencialidad); su art. 5° califica los datos biométricos como datos sensibles.
- **Ley Estatutaria 2573 de 2026:** medidas frente a la suplantación de identidad en telecomunicaciones, entidades financieras y establecimientos de comercio; revisada por la Sentencia C-413 de 2025.
- **Ley 2489 de 2025 y Decreto 769 de 2026** (adicionan el Decreto 1078 de 2015, arts. 2.2.31.2.4 a 2.2.31.2.6 y 2.2.31.3.3): modelo de verificación de edad para entornos digitales de niños, niñas y adolescentes basado en riesgo, minimización de datos, proporcionalidad y neutralidad tecnológica; confirman que los

proveedores no están obligados a ejercer funciones de policía judicial ni a transferir datos sin orden y reserva judicial.

- **Ley 906 de 2004, art. 244:** control judicial y reglas de acceso a información confidencial en investigaciones penales.
- **Ley 1480 de 2011, art. 50:** deberes de identificación del proveedor o expendedor en comercio electrónico.
- **Ley 1098 de 2006:** interés superior del menor y derecho progresivo a la participación.
- **Ley 599 de 2000, art. 269H:** circunstancias de agravación punitiva para los delitos informáticos del Título VII BIS, al que el art. 18° del proyecto agrega el numeral 9, aplicable cuando el delito se cometa mediante una cuenta o perfil que suministre información engañosa en la verificación de identidad.

Fuentes consultadas

- Sentencia C-413 de 2025 — relatoría oficial
- Sentencia SU-420 de 2019 — relatoría oficial
- Sentencia T-275 de 2021 — relatoría oficial
- Sentencia C-729 de 2000 — Función Pública
- Sentencia C-1011 de 2008 — SUIN-Juriscol
- Sentencia T-241 de 2023 — relatoría oficial
- Sentencia T-348 de 2026 — relatoría oficial
- Sentencia C-336 de 2007 — relatoría oficial
- Sentencia T-391 de 2007 — relatoría oficial
- Sentencia C-527 de 2003 — relatoría oficial
- Sentencia T-1157 de 2000 — relatoría oficial

VI. Impacto fiscal

De conformidad con el artículo 7° de la Ley 819 de 2003, el proyecto no ordena gasto público adicional ni crea una fuente de financiación distinta de las existentes. Las obligaciones centrales del articulado recaen sobre los proveedores de redes sociales y plataformas digitales, a su propio costo. Las entidades públicas que intervienen en su aplicación —la Registraduría Nacional del Estado Civil (una de las alternativas de verificación del art. 9°, no la única, desde que se incorporó la posibilidad de acreditar prestadores de confianza digital), la Superintendencia de Industria y Comercio y las demás autoridades sectoriales (art. 17°), y la Fiscalía General de la Nación y la rama judicial (Título V)— ejercen funciones ya asignadas por su régimen legal vigente; el

proyecto no les atribuye una función nueva, sino que precisa las condiciones de su ejercicio frente a la verificación de identidad digital.

VII. Competencia del Congreso y trámite

El Congreso de la República tiene competencia para expedir la presente ley en virtud de la cláusula general de competencia legislativa (art. 150 C.P.). Por su contenido, el proyecto desarrolla elementos estructurales, condiciones de ejercicio y garantías directamente vinculados con el núcleo del derecho a la intimidad y al habeas data (art. 15 C.P.) y de la libertad de expresión (art. 20 C.P.), lo que activa la reserva de ley estatutaria del artículo 152, literal a), de la Constitución Política (Marco Normativo, sección V).

En consecuencia, el proyecto se tramitará como ley estatutaria por la Comisión Primera Constitucional Permanente de la Cámara de Representantes, a la que corresponde el conocimiento de los proyectos de ley estatutaria y de los asuntos relacionados con derechos fundamentales (art. 2°, Ley 3ª de 1992), y estará sujeto a los requisitos propios de este trámite: aprobación por mayoría absoluta de los miembros de cada cámara, discusión dentro de una sola legislatura, y revisión previa de constitucionalidad por parte de la Corte Constitucional antes de la sanción presidencial (art. 153 C.P.).

VIII. Posibles conflictos de interés

En cumplimiento del artículo 291 de la Ley 5ª de 1992, modificado por el artículo 3° de la Ley 2003 de 2019, se describen a continuación las circunstancias o eventos que podrían generar un conflicto de interés en la discusión y votación de este proyecto, de acuerdo con el artículo 286 de esa misma ley.

Según el artículo 286 de la Ley 5ª de 1992, modificado por el artículo 1° de la Ley 2003 de 2019, existe conflicto de interés cuando la discusión o votación del proyecto pueda resultar en un beneficio particular, actual y directo a favor del congresista; se entiende por directo el beneficio que se produce de forma específica respecto del congresista, de su cónyuge, compañero o compañera permanente, o de sus parientes dentro del segundo grado de consanguinidad, segundo de afinidad o primero civil.

Este proyecto establece reglas de carácter general: obligaciones de verificación de identidad para los proveedores de redes sociales y plataformas digitales, garantías para los usuarios y condiciones para el acceso de las autoridades a la información de identidad. No crea beneficios, privilegios ni exenciones particulares a favor de un congresista determinado ni de las personas mencionadas, y sus efectos se extienden a todos los proveedores y usuarios comprendidos en su ámbito de aplicación.

A título de criterio orientador, podrían encontrarse en una situación de posible conflicto de interés los congresistas que, o cuyo cónyuge, compañero o compañera permanente o parientes dentro de los grados señalados, tengan un interés económico directo y actual en un proveedor de redes sociales o plataforma digital sujeto a esta ley, o en una empresa

que preste servicios de verificación de identidad, de atestación de atributos o de confianza digital, como los previstos en el artículo 9°, de manera que la aprobación del proyecto les genere un beneficio particular, actual y directo. Corresponde a cada congresista evaluar su situación y declararse impedido cuando considere que se configura una causal, sin perjuicio de otras que pueda advertir.

El autor manifiesta que no tiene conflicto de interés alguno frente a esta iniciativa.

Cordialmente,

MIGUEL ÁNGEL PINTO RUEDA
Representante a la Cámara por Santander

MIGUEL ÁNGEL PINTO RUEDA Representante a la Cámara ***Autor*** Departamento de Santander	**DANIEL BRICEÑO** Representante a la Cámara Bogotá ***Coautor***
MAURICIO TORO ORJUELA Representante a la Cámara Bogotá ***Coautor***	**Eimy Suárez González**

	Representante a la Cámara Norte de Santander ***Coautor***
JAIME ARIZABALETA FAJARDO Representante a la Cámara Departamento del Valle del Cauca Partido Centro Democrático	**JUAN DAVID LONDOÑO ARANGO** Representante a la Cámara Departamento de Vichada Partido de la U
MATEO HIDALGO MONTOYA Representante a la Cámara Caldas ***Coautor***	**MARTHA ISABEL RUIZ SOLERA** Representante a la Cámara Por Córdoba ***Coautor***