Anexo 1. Proyecto de Ley

PROYECTO DE LEY No. ___ de 2026

"Por medio de la cual se crea el Marco de Derechos Digitales, se establece el Constitucionalismo Digital Colombiano y se dictan otras disposiciones".

El Congreso de Colombia DECRETA:

EXPOSICIÓN DE MOTIVOS

La acelerada transformación digital derivada de la Quinta Revolución Industrial plantea retos inéditos para la protección de los derechos fundamentales, en especial frente a la masificación de tecnologías como la Inteligencia Artificial, el Big Data, el Blockchain, el Metaverso, la Robótica avanzada y los Ciber-robots. Estos avances ofrecen oportunidades de desarrollo económico y social, pero también generan riesgos relacionados con la privacidad, la identidad digital, la igualdad, la libertad de expresión, la seguridad jurídica y la dignidad humana.

En Colombia, el marco constitucional de 1991, si bien ha permitido proteger algunos derechos por conexidad, resulta insuficiente para abordar fenómenos tecnológicos emergentes. La jurisprudencia de la Corte Constitucional ha llenado vacíos puntuales, pero el país requiere una respuesta legislativa integral que anticipe riesgos, armonice innovación y derechos fundamentales, y consolide un verdadero Constitucionalismo Digital preventivo, ético y sostenible.

El presente proyecto de ley reconoce derechos digitales expresos, crea una institucionalidad robusta para su supervisión y garantiza la posibilidad de protegerlos mediante acción de tutela inmediata. Su objetivo es dotar al país de un marco normativo moderno, acorde con estándares internacionales y con la dignidad humana como eje central del Estado Social de Derecho.

TÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto. El objeto de esta ley es establecer un marco normativo integral para regular el uso de las tecnologías emergentes y la protección de los derechos digitales en Colombia,

garantizando una digitalización segura, inclusiva y justa para todos los ciudadanos. Esta ley define las obligaciones de las empresas tecnológicas, fortalece las capacidades de las autoridades para la supervisión de la digitalización, promueve nuevos derechos digitales, y establece sanciones y tipificaciones de delitos en el ámbito digital para prevalecer la privacidad, seguridad y libertad de quien la use.

Artículo 2. Definiciones. En la Quinta Revolución Industrial, las nuevas tecnologías son las siguientes:

1. **Metaverso:** Un espacio virtual en línea donde los usuarios pueden interactuar en un mundo tridimensional generado por computadora. Plantea desafíos para la privacidad y la libertad de expresión, ya que los usuarios pueden ser monitoreados y censurados por las empresas que controlan estas plataformas.

2. **Inteligencia Artificial (IA):** La IA se utiliza cada vez más en la toma de decisiones en áreas como empleo, justicia y salud, pero puede ser sesgada y discriminatoria, lo que plantea desafíos para la igualdad y la no discriminación.

3. **Big Data:** La recopilación y análisis de grandes cantidades de datos plantea riesgos para la privacidad y la protección de datos personales.

4. **Blockchain:** Tecnología de registro distribuido que crea sistemas de confianza y transparencia en línea, pudiendo ser utilizada para proteger la privacidad y seguridad de los datos personales.

5. **Teknización:** Integración creciente de la tecnología en la vida cotidiana, planteando retos para la privacidad y autonomía personal.

6. **Transhumanismo:** Movimiento que busca mejorar la condición humana a través de la tecnología, lo que plantea desafíos éticos y legales en torno a la identidad y la igualdad.

7. **Personas ciborg:** Personas que han integrado tecnología en su cuerpo, lo cual plantea retos para la privacidad y la autonomía personal.

Artículo 3. Alcance de la ley

1. Reconocer y garantizar los derechos digitales de las personas naturales y jurídicas en Colombia.
2. Establecer el marco jurídico del Constitucionalismo Digital Colombiano, alineado con los principios del Estado Social de Derecho y la Quinta Revolución Industrial.
3. Crear la Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA) y el Comité Nacional de Derechos Digitales y Tecnologías Emergentes.

Artículo 2. Principios rectores: La interpretación y aplicación de esta ley se guiará por los siguientes principios:

1. Dignidad humana y autonomía personal. La dignidad humana es el eje central del ordenamiento jurídico y se extiende a los entornos digitales, garantizando que ninguna persona sea reducida a un simple dato, perfil o algoritmo. La autonomía personal implica que cada individuo pueda ejercer control consciente sobre su información digital, sus decisiones tecnológicas y su identidad en entornos virtuales.

2. Legalidad y seguridad jurídica digital. Todo uso de tecnologías emergentes debe ajustarse a la ley, garantizando certeza sobre los derechos y obligaciones en entornos digitales. La seguridad jurídica digital protege a las personas y empresas frente a decisiones arbitrarias, vacíos normativos y riesgos derivados de la innovación tecnológica.

3. Neutralidad tecnológica. El Estado debe garantizar que ninguna plataforma, proveedor o tecnología sea favorecida o discriminada de manera injustificada. La neutralidad tecnológica asegura que el acceso a los servicios digitales no dependa del contenido, origen o destino de los datos, evitando censura o bloqueos arbitrarios.

4. Ética algorítmica y explicabilidad. Todo sistema automatizado, inteligencia artificial o algoritmo con impacto social debe desarrollarse y aplicarse conforme a criterios éticos, garantizando transparencia, auditabilidad y la posibilidad de explicar de manera comprensible las decisiones que afecten derechos de las personas.

5. Inclusión y acceso universal a las tecnologías. Toda persona tiene derecho a acceder, utilizar y beneficiarse de las tecnologías digitales sin discriminación por razones económicas, sociales, territoriales o culturales. La inclusión digital promueve la reducción de brechas tecnológicas y asegura la participación equitativa en la sociedad digital.

6. Prevención, precaución y proporcionalidad en la innovación. El desarrollo y adopción de tecnologías emergentes deberá anticipar y minimizar riesgos para los derechos fundamentales. Se aplicarán medidas preventivas y de precaución cuando exista incertidumbre sobre impactos potenciales, asegurando que toda limitación a derechos sea adecuada, necesaria y proporcional.

TÍTULO II. DERECHOS DIGITALES

Artículo 3. Derechos digitales. Se reconocen los siguientes derechos fundamentales para los ciudadanos en el entorno digital:

1. **Derecho a la privacidad digital:** Protección de la vida privada y los datos personales en el ámbito digital.

2. **Derecho a la protección de datos personales:** Derecho a decidir sobre el uso, acceso, tratamiento y circulación de los datos personales.

3. **Derecho a la seguridad digital:** Protección contra el acceso no autorizado a dispositivos y datos, y frente a vulnerabilidades o ataques digitales.

4. **Derecho a la accesibilidad digital:** Acceso equitativo a información, servicios y plataformas digitales, sin discriminación.

5. **Derecho a la libertad de expresión digital:** Derecho a expresar ideas y opiniones a través de medios digitales, respetando los derechos fundamentales de los demás.

6. **Derecho a la portabilidad de los datos:** Derecho de trasladar, transferir o mover los datos personales entre diferentes plataformas o servicios.

7. **Derecho a la educación digital:** Derecho a acceder a la formación necesaria para el uso seguro y ético de las tecnologías digitales.

8. **Derecho a la transparencia digital:** Derecho a recibir información clara sobre las políticas de privacidad y las prácticas de recolección de datos.

9. Derecho a la seguridad digital: Los usuarios de servicios de redes sociales y similares tienen derecho a la seguridad de sus comunicaciones a través de Internet, y los proveedores deben informar a los usuarios de sus derechos.

10. Derecho a la educación digital: El sistema educativo garantizará que los estudiantes aprendan a usar de forma segura y respetuosa los medios digitales, y que reciban educación sobre los riesgos derivados de la tecnología, incluyendo la violencia en línea.

11. Protección de menores de edad en Internet: Se garantizará que los menores usen los dispositivos digitales y servicios en línea de manera equilibrada y responsable. Se intervendrá en caso de difusión no autorizada de imágenes o datos personales de menores, protegiendo su dignidad y derechos fundamentales.

12. Derecho de rectificación en Internet: Las personas tienen derecho a rectificar contenidos falsos o erróneos difundidos en redes sociales y servicios en línea que atenten contra su honra, buen nombre o intimidad.

13. Derecho a la actualización de información en medios digitales: Toda persona tiene derecho a solicitar que los medios digitales incluyan un aviso de actualización

cuando la información ya publicada no refleje su situación actual, especialmente si hay decisiones judiciales o administrativas posteriores.

14. **Protección de datos de menores en Internet:** Las entidades que trabajen con menores deben garantizar la protección de sus datos personales, y obtener consentimiento previo de sus representantes legales para la difusión de dicha información en plataformas digitales.

15. **Derecho al olvido en búsquedas de Internet.** Las personas tienen derecho a que se eliminen enlaces de resultados de búsqueda que contengan información falsa, desactualizada o que ya no sea relevante para los fines para los que fue recopilada.

Artículo 4. Reconocimiento de derechos digitales por conexidad. Se reconocen como derechos fundamentales en entornos digitales, protegibles mediante acción de tutela inmediata, los siguientes:

1. **Derecho a la intimidad digital y habeas data digital**: Toda persona tiene derecho a que su información personal en entornos digitales sea recolectada, almacenada, procesada y compartida únicamente con su consentimiento expreso, respetando los principios de finalidad, proporcionalidad y seguridad. Incluye el derecho a conocer, actualizar, rectificar y suprimir datos personales de cualquier base de datos digital.

2. **Derecho a la identidad e imagen digital:** Consiste en la facultad de controlar la representación y uso de la imagen, voz, avatar o cualquier elemento que identifique digitalmente a una persona. Se prohíbe suplantar, alterar o manipular la identidad digital sin autorización, incluyendo el uso de deepfakes y tecnologías similares.

3. **Derecho a la igualdad y no discriminación algorítmica:** Toda persona tiene derecho a que las decisiones automatizadas o algorítmicas que le afecten se realicen sin sesgos discriminatorios por razones de raza, género, orientación sexual, origen social, situación económica, creencias o cualquier otra condición. La

discriminación derivada de algoritmos será considerada una vulneración de la igualdad ante la ley.

4. **Derecho a la libertad de expresión y acceso a Internet sin censura algorítmica:** Toda persona puede expresar, recibir y difundir información en entornos digitales sin restricciones indebidas ni bloqueos automatizados carentes de justificación legal. Se garantiza el acceso libre, plural y seguro a Internet como medio esencial para el ejercicio de derechos fundamentales.

5. **Derecho a la seguridad digital y protección frente a ciberdelitos.** Toda persona tiene derecho a la protección de sus sistemas, dispositivos, cuentas y comunicaciones personales frente a ataques cibernéticos, accesos no autorizados, fraudes, suplantaciones, extorsiones digitales o cualquier forma de vulneración que comprometa la integridad de su información o su seguridad personal.

Este derecho tendrá eficacia inmediata y transitoria, permitiendo la adopción de medidas cautelares digitales frente a las plataformas donde se haya cometido el ciberdelito, mientras la justicia penal adelanta la investigación correspondiente. Dichas medidas no sustituyen la actuación penal, sino que buscan proteger de manera preventiva al usuario afectado.

6. **Derecho a la desconexión digital y al descanso tecnológico:** Toda persona tiene derecho a limitar la interacción con herramientas digitales fuera de su jornada laboral o educativa, a no ser contactada de manera obligatoria en horarios de descanso, y a preservar espacios libres de hiperconectividad que garanticen su salud física y mental.

Artículo 5. Derechos digitales Personales. Se crean y reconocen como derechos digitales autónomos, complementarios a los derechos fundamentales:

1. **Propiedad intelectual digital y patrimonios virtuales:** Toda persona tiene derecho a la protección jurídica de sus creaciones, activos y bienes digitales, incluyendo obras digitales, software, datos originales, criptoactivos, NFTs y demás

patrimonios virtuales, con la posibilidad de transferirlos, licenciar su uso o disponer de ellos libremente.

2. **Muerte digital y derecho post-mortem a la desconexión:** Los titulares de cuentas, datos o activos digitales podrán definir su destino tras el fallecimiento, incluyendo su eliminación, conservación, transferencia o anonimización. La familia o herederos solo podrán acceder conforme a la voluntad digital previamente expresada por el titular.

3. **Sucesión digital y herencia tecnológica:** Los activos y patrimonios digitales forman parte de la sucesión del titular y podrán ser transmitidos a sus herederos bajo los mismos principios aplicables a la herencia material, con respeto a la privacidad y las licencias tecnológicas correspondientes.

4. **Reserva digital entre usuario y plataforma:** Los usuarios tienen derecho a que sus datos y contenidos alojados en plataformas digitales se utilicen exclusivamente para los fines autorizados, con prohibición de transferencias, análisis o monetización no consentida.

5. **Derecho a la integridad algorítmica:** Toda persona tiene derecho a que los sistemas automatizados que afecten su esfera personal, patrimonial o social operen con transparencia, trazabilidad y posibilidad de auditoría. Ninguna decisión algorítmica podrá ser inatacable o completamente opaca frente al usuario.

Artículo 6. Acción de tutela digital. Las vulneraciones o amenazas a los derechos reconocidos en los artículos anteriores podrán ser protegidas mediante acción de tutela digital, la cual procederá de manera inmediata o por conexidad con un derecho fundamental tradicional, garantizando la protección eficaz de la persona en entornos digitales y la restauración de su derecho afectado.

Artículo 7. Autoridad de Protección de Garantías de los Derechos Digitales. La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, garantizará el ejercicio de los derechos establecidos en esta ley.

TÍTULO III. DELITOS PENALES

Artículo 8. Incorpore al Código Penal de Colombia: Delitos de Ciberdelincuencia: En atención al creciente impacto de los delitos cibernéticos en nuestra sociedad, proponemos la inclusión y actualización de disposiciones específicas en el Código Penal colombiano para abordar eficazmente los siguientes delitos:

1. Robo de datos personales: Quien, sin autorización, obtenga, utilice, transfiera o comercialice datos personales de terceros, ya sea a través de técnicas de phishing, spyware, robo de datos financieros o cualquier otro medio informático, será sancionado con prisión de cinco (5) a diez (10) años y multa de cincuenta (50) a doscientos (200) salarios mínimos legales mensuales vigentes.

Circunstancias agravantes: Son eventos de agravaciones: Si los datos sustraídos pertenecen a menores de edad, personas mayores, o están relacionados con información financiera o de salud. Si se utiliza dicha información para extorsión, fraude de identidad o cualquier acto ilícito que cause daño económico o moral.

2. Delitos contra menores en entornos digitales: Quien utilice redes o medios digitales para: Difundir material pornográfico infantil, Acosar, amenazar o corromper a menores de edad, Participar en redes de trata de personas o desaparición de menores.
Será sancionado con prisión de diez (10) a veinte (20) años y multa de cien (100) a quinientos (500) salarios mínimos legales mensuales vigentes.

Circunstancias agravantes: Si el delito se comete utilizando plataformas de educación o herramientas diseñadas para proteger a los menores. Si se involucra a más de un menor de edad.

3. Piratería digital: Quien, sin autorización, reproduzca, distribuya o comercialice material protegido por derechos de autor mediante plataformas digitales,

será sancionado con prisión de tres (3) a ocho (8) años y multa de treinta (30) a cien (100) salarios mínimos legales mensuales vigentes.

Circunstancias agravantes: Si la distribución incluye obras inéditas o causa un perjuicio económico superior a quinientos (500) salarios mínimos legales mensuales vigentes. Si el responsable es parte de una red organizada para la piratería.

Artículo 9. Ciberseguridad y colaboración internacional. El Estado promoverá la construcción de un marco normativo integral de ciberseguridad, orientado a:

1. Fomentar alianzas multisectoriales entre entidades públicas, empresas privadas, organizaciones académicas y sociedad civil, con el fin de prevenir, detectar y mitigar los delitos cibernéticos.
2. Facilitar la cooperación y coordinación entre las fuerzas del orden nacionales e internacionales, mediante tratados, convenios y protocolos específicos, garantizando el intercambio oportuno de información en tiempo real y la adopción de acciones conjuntas frente a amenazas digitales.
3. Impulsar la protección proactiva de la infraestructura digital crítica, asegurando la continuidad de los servicios esenciales y la protección de los derechos digitales de la ciudadanía.

TÍTULO IV. INSTITUCIONALIDAD DIGITAL

Artículo 10. Creación de la Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA).

Créase la Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA) como una entidad técnica especializada, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con personería jurídica, autonomía administrativa, financiera y presupuestal, cuya finalidad será garantizar la protección integral de los derechos digitales, la seguridad en entornos tecnológicos y la gobernanza responsable de la inteligencia artificial y demás tecnologías emergentes.

Son funciones principales de la ANSDIA:

1. Supervisar y vigilar el cumplimiento de la presente ley y de las normas complementarias en materia de derechos digitales, ciberseguridad y gobernanza tecnológica.
2. Auditar, evaluar y certificar los sistemas algorítmicos y plataformas tecnológicas de alto riesgo, garantizando su transparencia, trazabilidad, explicabilidad y respeto por los derechos fundamentales.
3. Coordinar la prevención, identificación y mitigación de riesgos asociados al uso de inteligencia artificial, blockchain, big data, metaverso, ciber-robótica y demás tecnologías emergentes, en articulación con entidades nacionales e internacionales.
4. Imponer medidas preventivas, correctivas y sancionatorias, incluyendo la suspensión temporal de operaciones digitales, bloqueo de plataformas infractoras y la imposición de multas, conforme al régimen sancionatorio previsto en esta ley.
5. Emitir lineamientos, guías técnicas y protocolos de supervisión, promoviendo la innovación responsable y la seguridad jurídica digital para usuarios y empresas tecnológicas.

Artículo 10. Comité Nacional de Derechos Digitales y Tecnologías Emergentes.

Créase el Comité Nacional de Derechos Digitales y Tecnologías Emergentes como instancia de coordinación, articulación y asesoría en materia de política pública digital, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El Comité estará integrado por:

1. Un delegado del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), quien lo presidirá.
2. Un delegado de la Superintendencia de Industria y Comercio (SIC).
3. Un delegado de la Agencia Nacional del Espectro (ANE).
4. Un delegado del Ministerio de Justicia y del Derecho.
5. Un delegado de la Fiscalía General de la Nación.
6. Dos representantes del sector privado tecnológico, designados por el Gobierno Nacional.
7. Dos representantes de la sociedad civil digital y la academia, elegidos mediante convocatoria pública.

Funciones del Comité:

A. Asesorar y coordinar la formulación de políticas públicas y estrategias nacionales en materia de derechos digitales, ciberseguridad y tecnologías emergentes.

b) Recomendar medidas preventivas y regulatorias para garantizar la protección de los derechos digitales y la innovación responsable.

c) Articular la cooperación interinstitucional e internacional, facilitando el intercambio de información y mejores prácticas en gobernanza digital.

d) Emitir informes anuales sobre la evolución de los derechos digitales y la adopción de tecnologías emergentes en el país.

PARÁGRAFO. El Comité se reunirá de manera ordinaria dos (2) veces al año, y de forma extraordinaria cuando así lo convoque su Presidencia, para atender situaciones urgentes relacionadas con derechos digitales o riesgos tecnológicos emergentes.

TÍTULO V. DERECHOS Y DEBERES

Capítulo I. Empresas tecnológicas

Artículo 12. Definición y requisitos de las empresas tecnológicas. Para los efectos de la presente ley, se entenderá por empresa tecnológica toda persona jurídica, nacional o extranjera, que desarrolle, administre, preste o comercialice servicios basados en tecnologías emergentes, incluyendo, entre otros:

1. Plataformas digitales, redes sociales y aplicaciones de intermediación de bienes o servicios.
2. Sistemas de inteligencia artificial y algoritmos de toma de decisiones automatizadas que incidan en la esfera personal, social o patrimonial de los usuarios.
3. Servicios basados en blockchain, criptoactivos, NFTs y patrimonios virtuales.
4. Infraestructuras y servicios de big data, internet de las cosas (IoT), metaverso y realidades extendidas.
5. Servicios de ciberseguridad y ciberdefensa prestados a terceros.

Artículo 13. Requisitos habilitantes para realizar operaciones en el territorio colombiano.

Toda empresa tecnológica que pretenda desarrollar, administrar, comercializar o prestar servicios basados en tecnologías emergentes dentro del territorio colombiano deberá obtener

habilitación por parte de la Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA), para lo cual deberá cumplir los siguientes requisitos:

a) Registro formal en Colombia.

b) Contar con domicilio en el territorio nacional.

c) Estar debidamente inscrita en la Cámara de Comercio, incluyendo en su objeto social las actividades tecnológicas que pretenda desarrollar.

d) Designar representante legal o apoderado responsable ante la ANSDIA y las autoridades competentes.

e) Cumplimiento de estándares de seguridad y gestión de riesgos: Adoptar políticas internas de privacidad, ciberseguridad y gestión de datos alineadas con la normativa colombiana y estándares internacionales.

f) Contar con protocolos de prevención, detección y respuesta ante incidentes de ciberseguridad, certificados por auditoría interna o externa.

g) Implementar mecanismos de trazabilidad y transparencia en los sistemas algorítmicos y plataformas de alto impacto.

Compromisos de protección al usuario:

1. Establecer canales de atención efectivos para que los usuarios puedan ejercer sus derechos digitales y presentar reclamaciones.
2. Garantizar medidas para la protección de la privacidad, integridad y seguridad digital de los usuarios.
3. Comprometerse a respetar el derecho a la desconexión digital y la no discriminación algorítmica.

Reporte y supervisión

a) Someter sus operaciones, algoritmos y plataformas de alto riesgo a la supervisión y auditoría de la ANSDIA.

b) Reportar a la ANSDIA cualquier incidente de ciberseguridad, fuga de datos o vulneración de derechos digitales en un plazo máximo de setenta y dos (72) horas

c) Aceptar la revocatoria de la habilitación en caso de incumplimiento grave de la normativa vigente.

PARÁGRAFO PRIMERO. La Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA) expedirá el Registro de Operaciones Digitales a favor de las empresas tecnológicas que cumplan plenamente con los requisitos habilitantes establecidos en la presente ley.

Dicho registro será condición necesaria para iniciar o continuar operaciones en el territorio colombiano, y su vigencia, renovación y control estarán sujetos a la supervisión permanente de la ANSDIA, sin perjuicio de las responsabilidades civiles, administrativas o penales que correspondan por incumplimiento de la normativa aplicable.

PARÁGRAFO SEGUNDO. Ninguna empresa tecnológica podrá iniciar operaciones en Colombia sin haber obtenido la habilitación prevista en este artículo. La ANSDIA establecerá los procedimientos, plazos y estándares técnicos para la solicitud, renovación y eventual cancelación de la habilitación.

PARÁGRAFO TERCERO. La Autoridad Nacional de Supervisión Digital e Inteligencia Artificial (ANSDIA) estará facultada para realizar auditorías periódicas, visitas de supervisión y verificaciones técnicas sobre las empresas tecnológicas habilitadas, con el fin de constatar el cumplimiento de los requisitos establecidos en la presente ley.

Con base en los resultados de dichas supervisiones, la ANSDIA podrá otorgar, renovar, suspender o revocar la habilitación, garantizando en todo momento el debido proceso administrativo y la protección de los derechos digitales de los usuarios.

Capítulo II. Deberes de las empresas tecnológicas

Artículo 14. Deberes de las empresas tecnológicas frente a los usuarios.

Las empresas tecnológicas que operen en el territorio colombiano estarán obligadas a garantizar la protección integral de los derechos digitales de sus usuarios, cumpliendo con los siguientes deberes:

1. Garantizar la seguridad, confidencialidad y trazabilidad de los datos personales, de uso y de cualquier información generada por los usuarios, aplicando medidas técnicas y organizativas adecuadas para prevenir accesos no autorizados, pérdidas o alteraciones.

2. Informar de manera clara, precisa y oportuna a los usuarios sobre los términos y condiciones de uso, los riesgos asociados a las tecnologías utilizadas, así como cualquier cambio sustancial en la prestación de sus servicios.

3. Establecer canales eficaces y de fácil acceso para la presentación de quejas, reclamaciones y denuncias, que permitan la protección oportuna de los derechos digitales y la atención inmediata de incidentes de seguridad.

4. Respetar el derecho a la desconexión digital, absteniéndose de realizar comunicaciones invasivas o no consentidas, especialmente fuera de horarios laborales o en espacios de descanso, salvo autorización expresa del usuario.

Artículo 15. Deberes de las empresas tecnológicas frente al Estado.

Las empresas tecnológicas habilitadas para operar en el territorio nacional deberán cumplir con los siguientes deberes frente al Estado colombiano y sus autoridades competentes:

1. Colaborar activa y oportunamente con las autoridades competentes en la prevención, investigación y persecución de delitos cibernéticos, así como en la protección de la infraestructura digital crítica.

2. Reportar a la ANSDIA, dentro de un plazo máximo de setenta y dos (72) horas contadas a partir de su detección, cualquier incidente de ciberseguridad, filtración de datos o vulneración que pueda afectar a los usuarios, a terceros o a la seguridad nacional.

3. Someter periódicamente sus sistemas, algoritmos y plataformas críticas a auditorías técnicas y de seguridad realizadas por la ANSDIA o por terceros acreditados, para garantizar su transparencia, trazabilidad y confiabilidad.

4. Cumplir estrictamente las medidas preventivas, correctivas y sancionatorias que imponga la ANSDIA, asegurando la implementación de los ajustes requeridos para mitigar riesgos y prevenir futuras vulneraciones.

Capítulo III. Derechos y deberes de los usuarios

Artículo 16. Derechos de los usuarios de servicios tecnológicos.

Además de los derechos digitales consagrados en el Título II de la presente ley, los usuarios de servicios tecnológicos gozarán de los siguientes derechos específicos:

1. Derecho a la información digital clara y transparente: Recibir información veraz, suficiente, precisa y fácilmente comprensible sobre el uso, tratamiento y destino de sus datos, así como sobre el funcionamiento de algoritmos, sistemas automatizados o procesos tecnológicos que puedan afectar directa o indirectamente su esfera personal, patrimonial o social.

2. Derecho a revocar el consentimiento: Retirar en cualquier momento el consentimiento previamente otorgado para el tratamiento de sus datos personales o digitales, sin que ello implique perjuicio o limitación para el ejercicio de sus derechos.

3. Derecho a la reparación y compensación: Acceder a mecanismos administrativos, judiciales o tecnológicos de reparación, incluyendo la compensación económica o la restitución de derechos digitales, cuando se demuestre la vulneración o afectación de sus derechos por parte de empresas tecnológicas o terceros.

4. Derecho a la desindexación, anonimización o supresión de contenidos digitales: Solicitar la desindexación, anonimización o eliminación de información personal alojada en plataformas digitales, motores de búsqueda o entornos virtuales, cuando su mantenimiento implique riesgo para la dignidad humana, la privacidad, la integridad personal o la seguridad digital del usuario.

Artículo 17. Deberes de los usuarios de servicios tecnológicos.

Los usuarios de servicios, plataformas y herramientas digitales deberán cumplir con los siguientes deberes, orientados a la seguridad digital, la convivencia tecnológica y la prevención de riesgos cibernéticos:

1. Uso responsable y conforme a la ley.Utilizar los servicios tecnológicos de manera responsable, ética y respetuosa de la normativa vigente, absteniéndose de realizar conductas que afecten los derechos de terceros o el orden público digital.

2. Prohibición de conductas ilícitas. Evitar toda acción u omisión que constituya delito cibernético, facilite su comisión o implique el uso indebido de recursos digitales, plataformas o tecnologías emergentes.

3. Protección activa de la seguridad digital. Adoptar medidas razonables de protección sobre sus dispositivos, cuentas, contraseñas y credenciales de acceso, para prevenir accesos no autorizados, suplantaciones o vulneraciones de su información personal.

4. Deber de colaboración y reporte. Informar de manera oportuna y veraz a las plataformas correspondientes o a la autoridad competente sobre cualquier incidente de seguridad, intento de fraude o vulneración de derechos digitales del que tenga conocimiento.

Capítulo IV. Funciones del Estado colombiano

Artículo 18. Funciones del Estado en materia de derechos digitales y gobernanza tecnológica.

Corresponderá al Estado colombiano, a través de sus entidades competentes y en el marco de sus funciones constitucionales y legales, garantizar la protección integral de los derechos digitales y la seguridad del ecosistema tecnológico nacional, para lo cual desarrollará las siguientes funciones:

1. Garantía y protección de derechos digitales: Velar por el goce efectivo de los derechos digitales reconocidos en la presente ley, asegurando mecanismos administrativos, judiciales y tecnológicos que permitan su ejercicio y tutela efectiva.

2. Regulación, vigilancia y control: Regular, supervisar y sancionar la actividad de las empresas tecnológicas que operen en el territorio nacional, de conformidad con los procedimientos administrativos previstos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA), sin perjuicio de las responsabilidades civiles, penales o internacionales a que haya lugar.

3. Promoción de educación y cultura digital: Fomentar la alfabetización digital, la educación en ciberseguridad y el uso ético de la tecnología, orientando campañas de prevención de riesgos en línea y fortalecimiento de la ciudadanía digital.

4. Cooperación nacional e internacional: Impulsar la cooperación multisectorial y la colaboración internacional en ciberseguridad, protección de datos, ética

algorítmica y gobernanza digital, promoviendo tratados, convenios y redes de intercambio de información que fortalezcan la protección de los usuarios y la seguridad tecnológica del país.

5. Protección de la infraestructura digital crítica: Identificar, proteger y monitorear la infraestructura digital crítica, asegurando la continuidad de los servicios esenciales, la seguridad nacional y la resiliencia del ecosistema digital frente a ciberamenazas, ataques o desastres tecnológicos.

TÍTULO VI. RESPONSABILIDAD Y RÉGIMEN SANCIONATORIO

Artículo 19. Responsabilidad de las empresas tecnológicas.

Toda persona jurídica que opere desarrolle, administre o comercialice tecnologías emergentes en el territorio nacional será responsable de garantizar la protección de los derechos digitales y el cumplimiento de la presente ley. Para tal efecto, estará obligada a:

1. Garantizar transparencia, trazabilidad y seguridad digital en el tratamiento de datos, la operación de sistemas automatizados y la prestación de servicios tecnológicos.
2. Implementar auditorías y mecanismos de verificación periódica sobre sistemas de inteligencia artificial, blockchain y algoritmos de alto impacto, garantizando su explicabilidad y ausencia de sesgos discriminatorios.
3. Reportar incidentes de ciberseguridad o filtración de datos a la ANSDIA en un plazo máximo de setenta y dos (72) horas a partir de su detección.

Artículo 20. Procedimiento sancionatorio y régimen de sanciones. El incumplimiento de las obligaciones establecidas en la presente ley dará lugar a un procedimiento

administrativo sancionatorio adelantado por la ANSDIA, el cual se regirá por lo dispuesto en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).

a) El procedimiento contará con dos instancias administrativas: Primera instancia, a cargo de la Dirección de Supervisión de la ANSDIA, que expedirá la decisión inicial.

b) Segunda instancia, a cargo de la Dirección Jurídica o el Despacho de la Dirección General de la ANSDIA, que resolverá el recurso de apelación.

Las sanciones administrativas podrán consistir en:

- Multas hasta por cinco mil (5.000) SMMLV.
- Suspensión temporal de operaciones digitales en el territorio nacional.
- Bloqueo o restricción de acceso a plataformas o servicios digitales infractores.
- Compensación integral a las víctimas, sin perjuicio de las acciones civiles y penales a que haya lugar.

PARÁGRAFO. La imposición de sanciones administrativas no excluye la responsabilidad civil, penal o internacional que pueda derivarse de la infracción cometida.

TÍTULO VII. GOBERNANZA Y SEGUIMIENTO INTERINSTITUCIONAL DE LOS DERECHOS DIGITALES

Artículo 21. Creación y naturaleza del Comité Digital Interinstitucional.

Créase el Comité Digital Interinstitucional para la Protección y Promoción de los Derechos Digitales, como instancia técnica, consultiva y de coordinación interinstitucional, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El propósito exclusivo del Comité será:

1. Hacer seguimiento a la garantía y cumplimiento de los derechos digitales reconocidos en la presente ley.

2. Emitir directrices, lineamientos y parámetros técnicos y éticos orientados a la protección, promoción y fortalecimiento de dichos derechos.

3. Monitorear la evolución normativa, social y tecnológica de los derechos digitales en el país, emitiendo informes públicos y recomendaciones preventivas dirigidas al Estado y a la sociedad civil.

Artículo 22. Integración del Comité Digital Interinstitucional.

El Comité Digital Interinstitucional estará conformado por miembros gubernamentales, académicos y representantes de la sociedad civil, garantizando un enfoque interdisciplinario y plural en la protección y promoción de los derechos digitales.

1. Miembros gubernamentales:

1. Un delegado del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), quien ejercerá la Presidencia del Comité.

2. Un delegado de la Superintendencia de Industria y Comercio (SIC).

3. Un delegado de la Agencia Nacional del Espectro (ANE).

4. Un delegado del Ministerio de Justicia y del Derecho.

5. Un delegado de la Rama Judicial, designado por el Consejo Superior de la Judicatura, con experiencia acreditada en derecho constitucional o derechos fundamentales.

2. Miembros académicos y de la sociedad civil:

6. Un representante de universidades acreditadas con facultades de Derecho, Ingeniería, Filosofía o Ciencias Sociales, designado de forma rotativa cada dos (2) años.

7. Un abogado constitucionalista con experiencia en derechos digitales, seleccionado mediante convocatoria pública.

8. Un filósofo o sociólogo con experiencia en ética de la tecnología, comportamiento digital o gobernanza tecnológica.

9. Un representante de la sociedad civil con reconocida trayectoria en derechos digitales y ciberseguridad, elegido mediante convocatoria pública.

PARÁGRAFO PRIMERO: El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) será responsable de organizar, coordinar y garantizar la transparencia de los procesos de elección de los miembros académicos y de la sociedad civil que integren el Comité, asegurando la idoneidad técnica, ética y profesional de los seleccionados.

PARÁGRAFO SEGUNDO: El Comité podrá invitar, con voz pero sin voto, a expertos internacionales, representantes de empresas tecnológicas, centros de investigación y organismos multilaterales que puedan aportar conocimiento especializado para el fortalecimiento de los derechos digitales y la gobernanza tecnológica en el país

Artículo 23. Funciones del Comité Digital Interinstitucional.

El Comité Digital Interinstitucional ejercerá funciones exclusivamente consultivas y de seguimiento, orientadas a la protección, promoción y fortalecimiento de los derechos digitales reconocidos en la presente ley. Para tal efecto, desarrollará las siguientes funciones:

1. Monitorear y evaluar el cumplimiento efectivo de los derechos digitales, analizando su impacto social, jurídico y tecnológico en el país.

2. Emitir lineamientos, directrices y recomendaciones preventivas, dirigidas a entidades públicas, empresas tecnológicas y usuarios, con el fin de fortalecer la garantía y protección de los derechos digitales.

3. Definir parámetros éticos, sociales y de buenas prácticas para la adopción responsable y segura de tecnologías emergentes en Colombia.

4. Fomentar el diálogo interdisciplinario e intersectorial entre Estado, academia, sociedad civil y sector privado, promoviendo la gobernanza digital, la ética tecnológica y la cooperación interinstitucional.

5. Elaborar y publicar informes anuales sobre el estado de los derechos digitales en el país, incluyendo indicadores de cumplimiento y recomendaciones no vinculantes para la mejora continua de políticas públicas y prácticas privadas.

6. Promover programas permanentes de educación, formación y sensibilización ciudadana en derechos digitales, ética algorítmica, protección de datos y uso responsable de las tecnologías.

Artículo 24. Funcionamiento del Comité Digital Interinstitucional.

1. El Comité Digital Interinstitucional se reunirá de manera ordinaria dos (2) veces al año y de forma extraordinaria cuando así lo convoque su Presidencia.

2. Las decisiones y recomendaciones del Comité se adoptarán por mayoría simple de sus miembros con derecho a voto y tendrán carácter estrictamente consultivo y preventivo.

3. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ejercerá la Secretaría Técnica, responsable de la convocatoria a sesiones,

elaboración y custodia de actas, gestión documental y difusión pública de los informes emitidos por el Comité.

PARÁGRAFO PRIMERO. El Comité contará con el apoyo técnico de la ANSDIA para la recopilación de información, análisis de indicadores y elaboración de informes técnicos, sin que ello implique funciones sancionatorias, de control o de habilitación.

PARÁGRAFO SEGUNDO. El presupuesto necesario para el funcionamiento del Comité estará a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que garantizará los recursos logísticos, administrativos y técnicos requeridos para el cumplimiento de sus funciones.

PARÁGRAFO TERCERO. Los documentos, informes y estudios elaborados por el Comité podrán contar con el apoyo de grupos de investigación de universidades acreditadas y, cuando corresponda, ser validados por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias), con el fin de garantizar su rigurosidad técnica, científica y académica.

TÍTULO VIII. DISPOSICIONES FINALES

Artículo 25. Reglamentación.

El Gobierno Nacional, por conducto de las entidades competentes, expedirá la reglamentación necesaria para la implementación y cumplimiento de la presente ley dentro de un plazo máximo de doce (12) meses, contados a partir de su promulgación.

Artículo 26. Transitorio. Plazo de adecuación para las empresas tecnológicas.

Las empresas tecnológicas que, a la fecha de entrada en vigor de la presente ley, se encuentren operando en el territorio colombiano sin cumplir la totalidad de los requisitos habilitantes establecidos en esta norma, dispondrán de un plazo máximo de doce (12) meses para:

1. Acreditar ante la ANSDIA el cumplimiento de los requisitos de habilitación exigidos por la presente ley.

2. Ajustar sus políticas internas, protocolos de ciberseguridad, planes de mitigación de riesgos y mecanismos de atención a usuarios, conforme a lo previsto en esta ley y su reglamentación.

3. Registrar formalmente sus operaciones digitales ante la ANSDIA y, en el caso de empresas extranjeras, designar representante legal y domicilio en Colombia.

PARÁGRAFO. Durante el plazo de transición, la ANSDIA podrá emitir recomendaciones preventivas y requerimientos de adecuación, sin imponer sanciones administrativas, salvo en los casos de incumplimiento grave que ponga en riesgo los derechos digitales de los usuarios o la seguridad nacional.

Artículo 27. Vigencia y derogatorias.

La presente ley entrará en vigor a partir de la fecha de su promulgación y deroga todas las disposiciones que le sean contrarias.