



GACETA DEL CONGRESO

SENADO Y CÁMARA

(Artículo 36, Ley 5ª de 1992)

IMPRENTA NACIONAL DE COLOMBIA

www.imprenta.gov.co

ISSN 0123 - 9066

AÑO XXXIII - N° 233

Bogotá, D. C., miércoles, 13 de marzo de 2024

EDICIÓN DE 13 PÁGINAS

DIRECTORES:

GREGORIO ELJACH PACHECO

SECRETARIO GENERAL DEL SENADO

www.secretariasenado.gov.co

JAIME LUIS LACOUTURE PEÑALOZA

SECRETARIO GENERAL DE LA CÁMARA

www.camara.gov.co

RAMA LEGISLATIVA DEL PODER PÚBLICO

SENADO DE LA REPÚBLICA

PROYECTOS DE LEY

PROYECTO DE LEY NÚMERO 254 DE 2024 SENADO

por medio de la cual se formulan lineamientos de política pública para la seguridad digital de niños, niñas y adolescentes, se modifica la Ley 1146 de 2007, la Ley 599 de 2000 y se dictan otras disposiciones.

Bogotá D.C., marzo de 2024

Doctor
GREGORIO ELJACH PACHECO
Secretario General
Senado de la República
Ciudad

Asunto: Radicación del Proyecto de Ley "POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLÍTICA PÚBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS Y ADOLESCENTES, SE MODIFICA LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES".

Reciba un cordial saludo, Dr. Gregorio

En nuestra calidad de Congresistas de la República y en uso de las atribuciones que nos han sido conferidas constitucional y legalmente, respetuosamente nos permitimos radicar el siguiente Proyecto de Ley:

- Proyecto de Ley No. 254 de 2024 Senado "POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLÍTICA PÚBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS Y ADOLESCENTES, SE MODIFICA LA LEY 1146 DE 2007, LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES".

Cumpliendo con el pleno de los requisitos contenidos en la Ley 5 de 1992, le solicitamos se sirva dar inicio al trámite legislativo respectivo.

Cordialmente,

ANA PAOLA ACUDELO GARCÍA
Senadora de la República
Partido Político MIRA

MANUEL VIRGÜEZ PIRAQUIVE
Senador de la República
Partido Político MIRA

IRMA LUZ HERRERA RODRÍGUEZ
Representante a la Cámara por Bogotá
Partido Político MIRA

CARLOS EDUARDO GUEVARA
Senador de la República
Partido Político MIRA

PROYECTO DE LEY No. de 2024 Senado

"POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLÍTICA PÚBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS Y ADOLESCENTES, SE MODIFICA LA LEY 1146 DE 2007, LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES".

ARTÍCULO 1° Objeto. La presente ley tiene por objeto establecer los lineamientos generales para la formulación e implementación de una política pública para la seguridad digital de los niños, niñas y adolescentes. Esta política estará enfocada en la sensibilización, prevención y protección de niñas, niños y adolescentes frente a los delitos realizados a través de internet, inteligencia artificial, redes sociales, medios informáticos y dispositivos móviles. Además, se busca identificar, clasificar y tipificar nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos que afectan a los niños, niñas y adolescentes y a la población en general.

CAPÍTULO I. POLÍTICA PÚBLICA Y SUS LINEAMIENTOS

ARTÍCULO 2° Fines de la política pública. Son fines de la política pública que se adopta mediante esta Ley, sensibilizar, prevenir y proteger la integridad física y mental de las niñas, niños y adolescentes, frente a los delitos realizados a través del internet, redes sociales y medios informáticos, así como facilitar el restablecimiento de sus derechos.

ARTÍCULO 3° Principios orientadores. La política pública para la seguridad digital de los niños, niñas y adolescentes se fundamentará en el respeto y la garantía de los derechos y libertades consagrados en la Constitución Política, y en los principios de:

- Prevención. Se refiere a las acciones, campañas y acciones pedagógicas para prevenir que los niños, niñas y adolescentes sean víctimas de los delitos contra la libertad personal, la integridad, la formación sexual y el patrimonio económico, a través de medios electrónicos o informáticos.
- Pertinencia. La pertinencia se refiere a la capacidad de diseñar, adecuar e implementar acciones de acuerdo a los nuevos contextos, nuevas tecnologías de información, nuevas redes sociales o medios de comunicación.
- Coordinación, concurrencia y subsidiariedad. Se refiere al tipo de relación y cooperación entre los diferentes niveles de la Administración Pública.
- Articulación. Se refiere al compromiso conjunto de los actores que se encuentran relacionados con la formación, vida y convivencia de los menores de edad, padres de familia, tutores, familiares cercanos, profesores, entre otros.

ARTÍCULO 4° Lineamientos generales de la política pública. La política pública para la seguridad digital de los niños, niñas y adolescentes estará bajo la responsabilidad del Ministerio de Tecnologías de la Información y las Comunicaciones y en coordinación con la Fiscalía General de la Nación, el Instituto Colombiano de Bienestar Familiar, y otras entidades que por sus competencias puedan coadyuvar, se formulará conforme a los siguientes lineamientos

- Reconocer y caracterizar las prácticas y delitos más usuales que a nivel nacional se presentan en contra de niñas, niños y adolescentes, como el envío de imágenes de contenido sexual o "sexting", seducción o engaño de un adulto a un menor de edad o "grooming", extorsión sexual o "sexorsión", edición de imágenes sexuales o "morphing", ciberbullying, manipulación para

cometer suicidio, autolesión, entre otros, teniendo en cuenta el contexto normativo, la diversidad, la institucionalidad, la existencia de los distintos actores, los avances y limitaciones tecnológicas.

2. Generar y actualizar los mecanismos suficientes para fortalecer los medios de denuncia e información. Al respecto se deberá definir una ruta o guía institucional para la atención prioritaria de las niñas, niños y adolescentes víctimas de este tipo de delitos.
3. Establecer campañas de carácter preventivo y acciones pedagógicas de sensibilización, en el nivel nacional y/o territoriales, mediante las cuales se involucre a las instituciones educativas públicas y privadas, padres de familia y proveedores de redes y servicios de telecomunicaciones, programas de responsabilidad social empresarial, redes sociales, sitios web de uso compartido, entre otros.
4. Determinar la necesidad de recursos e identificar las fuentes de estos, disponibles para la inversión en campañas, acciones pedagógicas, sin perjuicio de las estrategias, programas y proyectos que actualmente se están ejecutando y conforme al trámite presupuestal.
5. A partir de un estudio de riesgos, establecer los departamentos y municipios a nivel nacional donde la política pública deba implementarse de manera prioritaria y en articulación con las autoridades territoriales correspondientes.
6. Implementar las acciones de manera tal que se faciliten la gestión de conocimientos, rendición de cuentas y monitoreo continuo en todos los niveles territoriales.
7. Incorporar en las estrategias todos los medios de comunicación institucional, incluyendo los mensajes cívicos dirigidos a realizar campañas pedagógicas de sensibilización y prevención de los crímenes cibernéticos contra niñas, niños y adolescentes.
8. Fortalecer la gestión del conocimiento, de los sistemas informáticos y tecnológicos para mejorar las investigaciones y estudios de la dinámica y el fenómeno de la explotación y/o violencia sexual contra los niños, niñas y adolescentes, tanto en el ámbito nacional como territorial; a su vez se propone la utilización.

Parágrafo 1° Los lineamientos, formulación, implementación y evaluación de la presente política pública se adelantarán según recomendaciones del Comité Nacional Interinstitucional constituido en la Ley 1336 de 2009 para la lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

Parágrafo 2° La política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes, se financiará con los recursos del Fondo contra la explotación sexual de menores creado en el artículo 24 de la Ley 679 de 2001. Los recursos del fondo se podrán utilizar para mejorar la gestión y pago por información que permita encontrar y romper con las cadenas y estructuras criminales dedicadas a la explotación sexual de menores.

ARTÍCULO 5° Sobre las campañas y acciones pedagógicas de la política pública. Las campañas y acciones pedagógicas, deberán lograr, sin perjuicio de otras consideraciones que formule el Comité Nacional Interinstitucional de la Ley 1336 de 2009 en el ejercicio de sus funciones:

1. Promover la construcción y consolidación de ambientes apropiados de convivencia en los entornos virtuales, a través del fortalecimiento de los planes institucionales del uso responsable de las TIC, con el fin de promover el manejo adecuado de Internet, la Inteligencia Artificial, las redes sociales y demás espacios informáticos.
2. Diseñar, implementar y desarrollar un sistema de gestión de la seguridad informática orientada a prevenir, detectar identificar, y reducir las posibilidades de delitos informáticos contra niñas, niños y adolescentes que cuente con un Plan Anual de Seguridad.

(120) meses.

Cuando la conducta sea cometida por los cónyuges o compañeros permanentes, aunque se hubieren separado o divorciado, la pena se aumentará hasta en una tercera parte.

No habrá lugar a responsabilidad penal cuando el agente utilice dichos contenidos con la intención de denunciar ante las autoridades competentes situaciones de agresión o acoso de las que ha sido o es víctima.

Artículo 9° Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 210C. Acoso virtual a menores de edad. El que, a través de internet, redes sociales, o cualquier otro medio o red de información, comunicación o sistema informático, contacte con un menor de edad y obtenga de este imágenes, grabaciones audiovisuales o cualquier representación de contenido sexual, o realice actos dirigidos a persuadir al menor para que participe en actividades sexuales, le facilite material de contenido sexual, o le muestre imágenes pornográficas donde se represente o aparezca un menor, incurrirá en pena de prisión de setenta y dos (72) a ciento veinte (120) meses, sin perjuicio de las demás sanciones penales a que hubiere lugar por el desarrollo de su conducta.

En la misma pena incurrirá quien, utilizando los mismos medios, contacte con un menor de edad y, mediante coacción, intimidación o engaño, busque obtener cualquier tipo de provecho sexual, sin perjuicio de las correspondientes por la comisión de otros delitos derivados de estas conductas.

Artículo 10° Adiciónese dos nuevos numerales al artículo 245 de la Ley 599 de 2000, el cual quedará así:

Artículo 245. Circunstancias de agravación.
(...)

12. Cuando el estreñimiento consiste en la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación, imágenes o grabaciones audiovisuales de la actividad sexual, o con contenido sexual de la víctima.
13. Cuando la conducta se cometa en persona menor de dieciocho (18) años.

Artículo 11. Adiciónese un nuevo artículo a la Ley 906 de 2004, el cual quedará así:

Artículo 91 A. Bloqueos de usuarios y dominios de internet. En cualquier momento a partir de la indagación, la Fiscalía General de la Nación podrá solicitar al juez de control de garantías que ordene a los proveedores de redes y servicios de telecomunicaciones, el bloqueo preventivo de los dominios de Internet, URL, cuentas y usuarios cuando existan motivos fundados que permitan inferir que, a través de aquellos, continuaría el desarrollo total o parcial de actividades delictivas en detrimento de los derechos de los niños, niñas y adolescentes.

El bloqueo se volverá definitivo cuando en la providencia que ponga fin al proceso resulte acreditada la materialidad de la infracción penal.

El funcionario judicial informará al Ministerio de Tecnologías de la Información y las Comunicaciones, o a quien haga sus veces, y a las demás autoridades competentes las decisiones de bloqueo, preventivo o definitivo, para lo de su competencia.

Parágrafo. El bloqueo preventivo o definitivo de los dominios de internet, URL, cuentas y usuarios deberá atender el principio de proporcionalidad, de manera tal que no vulnere derechos

Parágrafo 1. De igual forma, el Ministerio de Tecnologías de la información y comunicaciones reglamentará que por lo menos el 1% de los mensajes comerciales o publicitarios de las empresas de telefonía móvil se destinen a la prevención y líneas de denuncia frente a posibles crímenes cibernéticos.

ARTÍCULO 6° Acciones complementarias. El Ministerio de Educación Nacional deberá formular guías para que las instituciones educativas a nivel nacional puedan implementar las siguientes acciones:

1. Fomentar la formación de la comunidad educativa para la identificación y denuncia de posibles casos o delitos contra niñas, niños y adolescentes.
2. Impulsar la creación de herramientas pedagógicas e informáticas para hacer de las instituciones educativas espacios que brinden a las niñas, niños y adolescentes protección y seguridad frente a eventuales casos de delitos informáticos.
3. Con el apoyo de la Policía Nacional, realizará una publicación bimestral con información sobre las modalidades delictivas que se han detectado, las conductas que pueden poner en riesgo a los niños, niñas y adolescentes y las acciones preventivas y la ruta de atención.
4. Evitar que personas condenadas por cometer cualquiera de los delitos contra la libertad, integridad y formación sexual, contemplados en el Código Penal Colombiano contra menores de edad, ejerzan cargos, empleos, oficios o profesiones en ámbitos educativos, de cuidado, de transporte escolar o de formación pública o privada que involucren una relación directa y habitual con menores de edad en cualquiera de sus grados.

ARTÍCULO 7° Modifíquese el artículo 15° de la Ley 679 de 2001 en los siguientes términos:

Artículo 15° SISTEMA DE INFORMACIÓN SOBRE DELITOS SEXUALES CONTRA MENORES. Para la prevención de los delitos sexuales contra menores de edad y el necesario control sobre quienes los cometen, promuevan o faciliten, el Ministerio de Justicia y del Derecho, la Policía Nacional de Colombia, el Instituto Colombiano de Bienestar Familiar y la Fiscalía General de la Nación desarrollarán un sistema de información en el cual se disponga de una completa base de datos sobre delitos contra la libertad, el pudor y la formación sexual cometidos sobre niños, niñas y adolescentes y aquellos que se cometen a través de medios informáticos o electrónicos contra menores de 18 años, sus autores, cómplices, proxenetas, tanto de condenados. La Policía Nacional de Colombia y la Fiscalía General de la Nación promoverán la formación de un servicio nacional e internacional de información sobre personas sindicadas o condenadas por delitos contra la libertad, el pudor y la formación sexual sobre niños, niñas y adolescentes. Para tal efecto se buscará el concurso de los organismos de policía internacional y se tendrán en cuenta las circulares de alerta que expide la Organización Internacional de Policía Criminal-INTERPOL.

CAPÍTULO II. DISPOSICIONES PENALES

Artículo 8° Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

Artículo 210B. Difusión no consentida de imágenes con contenido sexual. El que, con el fin de satisfacer sus deseos o los de un tercero o con la intención de castigar o silenciar publique, divulgue o revele, a través de cualquier medio o red de información o de comunicación, imágenes o grabaciones audiovisuales, o imágenes o videos generados artificialmente de la actividad sexual o con contenido sexual de una persona, sin su autorización, incurrirá en prisión de setenta y dos (72) a ciento veinte

fundamentales como el de libertad de expresión y acceso a la información. Sobre esta decisión procede el recurso de reposición y de apelación.

CAPÍTULO III. DISPOSICIONES FINALES.

Artículo 12° Modifíquese el artículo 3° de la Ley 1146 de 2007 de la siguiente manera:

Artículo 3°. De su creación. Créase adscrito al Ministerio de Salud y Protección Social, el Comité Interinstitucional Consultivo para la Prevención de la Violencia Sexual y Atención Integral de los Niños, Niñas y Adolescentes Víctimas del Abuso Sexual, mecanismo consultivo de coordinación interinstitucional y de interacción con la sociedad civil organizada, conformado por:

1. Ministerio de Salud y Protección Social, o su delegado, quien lo presidirá.
2. Ministerio de Educación Nacional, o su delegado.
3. Ministro de las Tecnologías de la Información y de las Comunicaciones, o su delegado.
4. Ministro de Justicia y del Derecho o su delegado.
5. Ministro de Relaciones Exteriores o el Director de Asuntos Consulares y de Comunidades Colombianas en el Exterior o su delegado.
6. Ministro de Comercio, Industria y Turismo o su delegado.
7. Director del Instituto Colombiano del Bienestar Familiar quien ejercerá la Secretaría Técnica.
8. Fiscal General de la Nación, o su delegado.
9. Procurador General de la Nación, o su delegado.
10. Defensor del Pueblo, o su delegado.
11. Director del Instituto Nacional de Medicina Legal y Ciencias Forenses.
12. Director general de la Policía Nacional o quien delegue.
13. Representante de la Comisión Reguladora de Comunicaciones o su delegado.
14. El Subdirector General de la Oficina de Interpol en Colombia o su delegado.
15. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - coCERTo su delegado.
16. Consejería Presidencial para la Niñez y Adolescencia o su delegado.
17. Consejería Presidencial para los Derechos Humanos y Asuntos Internacionales o su delegado.
18. Consejería presidencial para asuntos económicos y transformación digital.
19. Un representante de las Asociaciones Colombianas de Psiquiatría, Psicología,
20. Pediatría, Sexología, quien será elegido entre ellas por cooptación y cuya participación será rotativa de conformidad con lo dispuesto por los Estatutos que regirán el Consejo.
21. Un (1) representante de las organizaciones no gubernamentales que tengan por finalidad la prestación de servicios de protección de los niños, niñas y adolescentes, que será elegido entre ellas por cooptación y cuya participación será rotativa de conformidad con lo dispuesto por los Estatutos que regirán el Consejo.

Parágrafo 1°. El Comité Interinstitucional Consultivo para la Prevención de la Violencia Sexual y Atención Integral de los Niños, Niñas y Adolescentes Víctimas del Abuso Sexual, cuyo carácter será permanente, podrá invitar a participar en relación con los temas de su competencia, con voz pero sin voto, a miembros de la comunidad universitaria y científica y a los observatorios sobre asuntos de género y organismos de cooperación internacional.

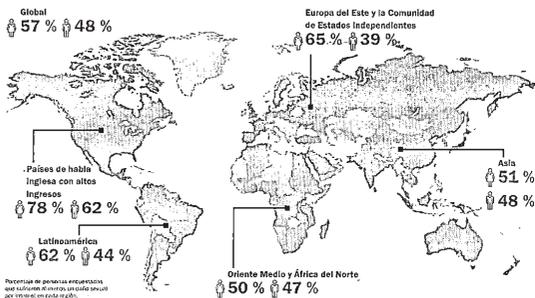
tendencias emergentes amenazan con incrementar aún más el volumen y la complejidad de los casos, agravando los retos de quienes trabajan para reducir el peligro y los daños. En cuanto al ciberacoso, se detectó que en mayo de 2021, la Europol desmanteló una página web de abuso sexual infantil de la Dark Web con más de 400 000 suscriptores. Hay más de 3 000 000 de cuentas registradas en las 10 páginas más dañinas sobre abuso sexual infantil de la Dark Web. Por término medio, 30 analistas del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) procesan cada día 60 000 denuncias en línea de abuso sexual infantil a través de la CyberTipline.

En el mismo estudio, se encontraron algunos datos clave, el 54 % de los encuestados ha sufrido al menos un daño sexual online durante su infancia, el 29 % recibieron contenido sexualmente explícito de un adulto conocido o desconocido antes de cumplir 18 años, el 25 % afirmó que un adulto conocido o desconocido les pidió que mantuvieran en secreto parte de sus interacciones sexuales explícitas en línea, el 29 % afirmó que alguien compartió imágenes o vídeos sexualmente explícitos de los menores sin permiso.

En las siguientes gráficas, se detalla el porcentaje a nivel global de los niños que sufren daños sexuales en internet (gráfica 1) y el porcentaje de los daños sexuales a menores por continente (gráfica 2).

Gráfica 1.

CASI LA MITAD DE LOS NIÑOS ha sufrido al menos un daño sexual en Internet.



sitios web falsos y campañas de recaudación de fondos fraudulentas. Este oportunismo subraya la naturaleza depredadora de los ciberdelincuentes, siempre listos para explotar las tragedias humanitarias para su propio beneficio.

A pesar de la atención centrada en los conflictos geopolíticos, la explotación sexual infantil en línea continúa siendo una amenaza persistente y creciente, con delincuentes explotando plataformas digitales para perpetrar abusos. Este crimen, profundamente perturbador, destaca la necesidad de una vigilancia constante y la cooperación internacional para proteger a los más vulnerables de nuestra sociedad.

El informe también arroja luz sobre la compleja red de servicios de cibercrimen, desde la venta de acceso inicial hasta la ofuscación de cargas maliciosas, que facilitan una amplia gama de actividades ilícitas, incluidos ataques de ransomware y esquemas de fraude. La interconexión de estos servicios muestra un ecosistema criminal bien organizado y altamente especializado, lo que plantea desafíos significativos para su detección y desmantelamiento.

El fenómeno de la toma de control de cuentas (ATO) se identifica como una técnica cada vez más común, aprovechando la abundancia de datos personales robados disponibles en los mercados negros. Esta práctica no solo conduce a pérdidas financieras directas para las víctimas, sino que también facilita otros crímenes, como el lavado de dinero y la extorsión.

La victimización múltiple emerge como un tema recurrente, con individuos y organizaciones enfrentando ataques sucesivos o simultáneos, lo que subraya la importancia de robustas estrategias de ciberseguridad y la concienciación sobre la seguridad en línea. Este ciclo de re-victimización es facilitado por la reutilización de credenciales comprometidas y la explotación de vulnerabilidades no parcheadas.

Las comunidades subterráneas en la dark web juegan un papel crucial en el reclutamiento y entrenamiento de nuevos ciberdelincuentes, así como en la facilitación del intercambio de tácticas, técnicas y procedimientos criminales. La existencia de estos foros refleja una cultura del cibercrimen que es a la vez resiliente y evolutiva, adaptándose constantemente a los esfuerzos de aplicación de la ley.

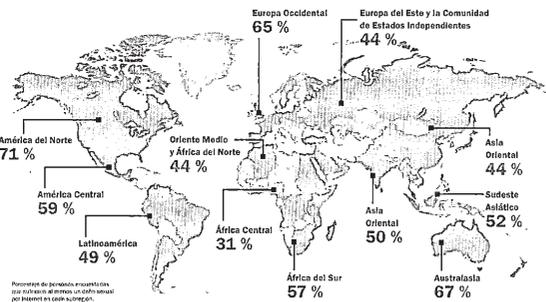
Finalmente, el informe también señala que el lavado de dinero de las ganancias criminales ilustra la sofisticación financiera de las redes de cibercrimen, empleando una mezcla de criptomonedas, plataformas de juego en línea y mulas de dinero para ocultar el origen ilícito de sus fondos. Este aspecto del cibercrimen no solo subraya la importancia de la cooperación transfronteriza, sino que también resalta la necesidad de regulaciones financieras más estrictas para combatir el flujo de dinero sucio a través de la economía digital.

El "Informe Anual 2022"¹⁰ de INTERPOL ofrece una perspectiva detallada y alarmante sobre la ciberdelincuencia a nivel global, poniendo especial énfasis en los delitos cometidos contra menores de edad en el ciberespacio. Este documento, fruto de la colaboración internacional y el análisis exhaustivo de incidentes reportados, destaca la creciente sofisticación y alcance de las redes criminales que operan en línea, así como la urgente necesidad de fortalecer las medidas de protección para los más vulnerables de nuestra sociedad.

¹⁰ https://www.interpol.int/es/content/download/19843/file/INTERPOL%20%20Anual%20Report%202022_SP.pdf

Gráfica 2.

Los daños sexuales en Internet a menores SUCEDEN EN TODOS LADOS...



De otro lado, señala la EUROPOL que "El creciente número de niños y adolescentes que poseen teléfonos inteligentes ha sido acompañado por la producción de material indecente autogenerado. Tal material, inicialmente compartido con intenciones inocentes, a menudo llega a los "recolectores", quienes a menudo proceden a explotar a la víctima, en particular mediante extorsión"⁸. El "Internet Organised Crime Threat Assessment (IOCTA) 2023"⁹ proporciona un análisis exhaustivo de las amenazas emergentes y persistentes en el ámbito del ciberdelito, destacando la ingeniosidad y adaptabilidad de los ciberdelincuentes ante el cambiante panorama tecnológico y socioeconómico global. Este informe, compilado por Europol, sirve como una llamada de atención para individuos, empresas y gobiernos sobre la creciente sofisticación y alcance de las actividades ilícitas en línea.

Uno de los hallazgos más alarmantes se refiere a la escalada de ciberataques políticamente motivados, especialmente en el contexto de la invasión de Ucrania por Rusia. Estos ataques no solo han revelado las divisiones políticas dentro de la comunidad ciberdelincente, sino que también han demostrado la capacidad de estos actores para desestabilizar infraestructuras críticas y socavar la seguridad nacional a través de campañas de desinformación y ataques disruptivos, destacando la geopolítica como un nuevo campo de batalla en el ciberespacio.

La crisis en Ucrania también ha alimentado una ola de fraudes en línea, con estafadores aprovechando la situación para engañar a los donantes bienintencionados mediante la creación de

⁸ <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>

⁹ https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

Los hallazgos del informe revelan un aumento preocupante en la cantidad y gravedad de los delitos cibernéticos, con especial atención a aquellos dirigidos contra menores. La Base de Datos Internacional de INTERPOL sobre Explotación Sexual de Niños (ICSE) ha permitido la identificación de 32,700 víctimas y la identificación de 14,500 delincuentes, con una media de 7 víctimas identificadas cada día. Además, INTERPOL ha realizado operaciones significativas contra la ciberdelincuencia, incluyendo la coordinación de esfuerzos en 27 países contra la ciberdelincuencia en África, resultando en la detención de 11 personas y la acción contra más de 200,000 fragmentos de infraestructuras de malware.

Las estadísticas indican un panorama sombrío donde la explotación sexual infantil en línea y el acoso cibernético emergen como amenazas significativas, exacerbadas por el anonimato y la omnipresencia del internet. Una operación policial internacional, apoyada por INTERPOL, desmanteló una red transnacional dedicada a la extorsión sexual, resultando en la detención de 12 sospechosos principales. Estos delitos no solo representan una violación a los derechos fundamentales de los niños, sino que también exponen las profundas cicatrices psicológicas y emocionales que afectan a las víctimas y sus familias. Este panorama destaca la importancia de la cooperación internacional y el uso de tecnología avanzada para proteger a los menores y perseguir a los responsables.

El informe subraya la necesidad imperiosa de una acción coordinada y decidida por parte de las autoridades globales, la industria tecnológica y las organizaciones de la sociedad civil para combatir estas atrocidades. Se hace un llamado a mejorar los sistemas de detección y respuesta a los delitos en línea, así como a promover una mayor educación y concienciación sobre la seguridad en internet entre los jóvenes y sus cuidadores.

INTERPOL, en su compromiso con la lucha contra la ciberdelincuencia, destaca la importancia de fortalecer las redes de cooperación internacional, compartir mejores prácticas y desarrollar herramientas innovadoras que permitan prevenir, detectar y responder de manera efectiva a los delitos cibernéticos. La organización reconoce los desafíos que presenta el dinámico entorno digital, pero se mantiene firme en su determinación de proteger a los ciudadanos, especialmente a los menores, de las amenazas que surgen en el ciberespacio.

5. IMPACTO ACTUAL DE CRÍMENES CIBERNÉTICOS EN COLOMBIA

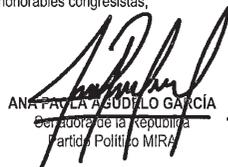
Según cifras de 2021, y de acuerdo a los procesos investigativos desarrollados por el Centro Cibernético Policial¹¹, estas son las aplicaciones de mayor uso para la distribución de Material de Abuso Sexual Infantil: Whatsapp, Telegram, Facebook, Snapchat, e Instagram.

Así mismo, El "BALANCE DE CIBERSEGURIDAD 2023"¹² Proporciona una visión integral de la situación de ciberseguridad, destacando la evolución y las tendencias de los delitos informáticos, así como los esfuerzos realizados para contrarrestar estos desafíos. A continuación, se presentan las principales cifras y hechos destacados del documento, estructurados en una narrativa coherente y contextualizada:

El informe revela un escenario preocupante en el ámbito de la ciberseguridad, con un incremento notable en el número de incidentes cibernéticos, reflejando la persistente amenaza que representan para individuos, empresas y entidades gubernamentales. Entre las modalidades de delitos informáticos más destacadas, se encuentran el phishing, con 6,804 incidentes, evidenciando una disminución del 12% en comparación con el año anterior, y las estafas relacionadas con la compra y/o venta de

¹¹ <https://drive.google.com/file/d/1JqXb5Avf0-vsKhSFA7zrYCWk-WFT2CBU/view?usp=sharing>

¹² https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

<p>responsabilidad de desarrollar estrategias nacionales para la prevención de delitos cibernéticos contra menores y realizar estudios que permitan comprender mejor las causas, consecuencias y métodos de prevención de estos delitos, enfatizando la importancia de una aproximación basada en evidencia y colaboración intersectorial.</p> <p>Finalmente, el artículo 14 establece que la ley entrará en vigencia inmediatamente después de su sanción y publicación, asegurando que las disposiciones contenidas en ella se apliquen de manera efectiva para fortalecer la protección de menores en el entorno digital, derogando cualquier normativa previa que contravenga los objetivos y principios establecidos en este proyecto de ley.</p> <p>7. CONSTITUCIONALIDAD Y LEGALIDAD</p> <p>Frente a la materia, es válido resaltar que el legislador cuenta con un amplio margen de libertad en la configuración normativa de la política criminal y de los procedimientos aplicables, que le permite adoptar medidas razonables para garantizar otros fines constitucionales. Las medidas penales y de procedimiento adoptadas para hacer frente a la ciberdelincuencia cumplen con estos requisitos constitucionales.</p> <p>Ahora bien, dentro del marco normativo colombiano se encuentran el sustento constitucional y legal de la presente iniciativa, que otorga una sobresaliente protección a los derechos de las niñas, niños y adolescentes, a nivel constitucional la Carta Política de 1991 dispone los siguientes:</p> <p>Artículo 1°. Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general.</p> <p>Artículo 2°. Son fines esenciales del Estado. Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.</p> <p>Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.</p> <p>Artículo 44. Son derechos fundamentales de los niños: la vida, la integridad física, la salud y la seguridad social, la alimentación equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado y amor, la educación y la cultura, la recreación y la libre expresión de su opinión. Serán protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos.</p> <p>Gozarán también de los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia. La familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral, y el ejercicio pleno de sus derechos. Cualquier persona puede exigir de la autoridad competente su cumplimiento y la sanción de los infractores. Los derechos de los niños prevalecen sobre los derechos de los demás.</p>	<p>Artículo 45. El adolescente tiene derecho a la protección y a la formación integral. El Estado y la sociedad garantizan la participación activa de los jóvenes en los organismos públicos y privados que tengan a cargo la protección, educación y progreso de la juventud. A nivel legal se identifican varias leyes que se dirigen específicamente a la prevención de delitos sexuales contra niñas, niños y adolescentes, en las que se encuentran:</p> <p>Ley 679 de 2001 por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.</p> <p>Artículo 4°. Comisión de Expertos. Dentro del mes siguiente a la vigencia de la presente ley, el Instituto Colombiano de Bienestar Familiar conformará una Comisión integrada por peritos jurídicos y técnicos, y expertos en redes globales de información y telecomunicaciones, con el propósito de elaborar un catálogo de actos abusivos en el uso y aprovechamiento de tales redes en lo relacionado con menores de edad. La Comisión propondrá iniciativas técnicas como sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos perjudiciales para menores de edad en las redes globales, que serán transmitidas al Gobierno nacional con el propósito de dictar medidas en desarrollo de esta ley.</p> <p>Artículo 12. Medidas de sensibilización. Las autoridades de los distintos niveles territoriales y el Instituto Colombiano de Bienestar Familiar, implementarán acciones de sensibilización pública sobre el problema de la prostitución, la pornografía y el abuso sexual de menores de edad. El Gobierno nacional, por intermedio del Ministerio de Educación, supervisará las medidas que a este respecto sean dictadas por las autoridades departamentales, distritales y municipales.</p> <p>Parágrafo 1°. Por medidas de sensibilización pública se entiende todo programa, campaña o plan tendiente a informar por cualquier medio sobre el problema de la prostitución, la pornografía con menores de edad y el abuso sexual de menores de edad; sobre sus causas y efectos físicos y psicológicos y sobre la responsabilidad del Estado y de la sociedad en su prevención.</p> <p>Artículo 15. Sistema de información sobre delitos sexuales contra menores. Para la prevención de los delitos sexuales contra menores de edad y el necesario control sobre quienes los cometen, promuevan o facilitan, el Ministerio de Justicia y del Derecho, el Departamento Administrativo de Seguridad, DAS, el Instituto Colombiano de Bienestar Familiar y la Fiscalía General de la Nación desarrollarán un sistema de información en el cual se disponga de una completa base de datos sobre delitos contra la libertad, el pudor y la formación sexuales cometidos sobre menores de edad, sus autores, cómplices, proxenetas, tanto de condenados como de sindicados.</p> <p>Ley 1098 de 2006, por la cual se expide el Código de la Infancia y la Adolescencia</p> <p>Artículo 18. Derecho a la integridad personal. Los niños, las niñas y los adolescentes tienen derecho a ser protegidos contra todas las acciones o conductas que causen muerte, daño o sufrimiento físico, sexual o psicológico. En especial, tienen derecho a la protección contra el maltrato y los abusos de toda índole por parte de sus padres, de sus representantes legales, de las personas responsables de su cuidado y de los miembros de su grupo familiar, escolar y comunitario.</p> <p>Ley 1336 de 2009, por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.</p> <p>Artículo 24. El artículo 218 de la Ley 599 quedará así:</p> <p>Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, transmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor</p>
<p>de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro. La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.</p> <p>Asimismo, el país cuenta con normatividad para proteger a las niñas, niños y adolescentes del ciberacoso o cyberbullying y otros tipos de violencia escolar, ejemplo de ello es la Ley 1620 de 2013 "por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar", que dispone:</p> <p>Artículo 2°. En el marco de la presente ley se entiende por:</p> <p>Competencias ciudadanas: Es una de las competencias básicas que se define como el conjunto de conocimientos y de habilidades cognitivas, emocionales y comunicativas que, articulados entre sí, hacen posible que el ciudadano actúe de manera constructiva en una sociedad democrática.</p> <p>Educación para el ejercicio de los derechos humanos, sexuales y reproductivos: Es aquella orientada a formar personas capaces de reconocerse como sujetos activos titulares de derechos humanos, sexuales y reproductivos con la cual desarrollarán competencias para relacionarse consigo mismo y con los demás, con criterios de respeto por sí mismo, por el otro y por el entorno, con el fin de poder alcanzar un estado de bienestar físico, mental y social que les posibilite tomar decisiones asertivas, informadas y autónomas para ejercer una sexualidad libre, satisfactoria, responsable y sana en torno a la construcción de su proyecto de vida y a la transformación de las dinámicas sociales, hacia el establecimiento de relaciones más justas, democráticas y responsables.</p> <p>Acoso escolar o bullying: Conducta negativa, intencional metódica y sistemática de agresión, intimidación, humillación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra un niño, niña, o adolescente, por parte de un estudiante o varios de sus pares con quienes mantiene una relación de poder asimétrica, que se presenta de forma reiterada o a lo largo de un tiempo determinado.</p> <p>También puede ocurrir por parte de docentes contra estudiantes, o por parte de estudiantes contra docentes, ante la indiferencia o complicidad de su entorno. El acoso escolar tiene consecuencias sobre la salud, el bienestar emocional y el rendimiento escolar de los estudiantes y sobre el ambiente de aprendizaje y el clima escolar del establecimiento educativo.</p> <p>Cyberbullying o ciberacoso escolar: Forma de intimidación con uso deliberado de tecnologías de información (internet, redes sociales virtuales, telefonía móvil y videojuegos online) para ejercer maltrato psicológico y continuado.</p> <p>De otra parte, el marco legal colombiano otorga herramientas para proteger la información y los datos personales, aspecto que es protegido a través de la sanción penal, como se establece en los siguientes tipos penales:</p> <p>Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".</p> <p>Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio</p>	<p>o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.</p> <p>Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.</p> <p>Finalmente, se tiene la Ley 1928 de 2016 por medio de la cual Colombia se adhirió al convenio sobre la ciberdelincuencia "Convenio de Budapest".</p> <p>8. IMPACTO FISCAL.</p> <p>De conformidad con el artículo 7° de la Ley 819 de 2003, los gastos que genere la presente iniciativa se entenderán incluidos en los presupuestos y en el Plan Operativo Anual de Inversión de la entidad competente. Es relevante mencionar, para el caso en concreto, que no obstante lo anterior tenemos como sustento un pronunciamiento de la Corte Constitucional, en la Sentencia C-911 de 2007, en la cual se puntualizó que el impacto fiscal de las normas, no puede convertirse en óbice, para que las corporaciones públicas ejerzan su función legislativa y normativa.</p> <p>Cabe resaltar que la iniciativa busca que las herramientas y autoridades existentes se articulen, unifiquen y mejoren las estrategias de protección de los niños, niñas y adolescentes ante los delitos realizados a través de medios informáticos o electrónicos.</p> <p>Es por todo lo anteriormente expuesto que los Congresistas abajo firmantes, nos permitimos poner a consideración del honorable Congreso de la República el presente texto, y le solicitamos tramitar y aprobar el proyecto de ley "Por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niñas, niños y adolescentes, se modifica el Código Penal y se dictan otras disposiciones".</p> <p>De los honorables congresistas,</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="876 2035 1104 2202">  ANA PAULA BUEDLO GARCÍA Senadora de la República Partido Político MIRA </div> <div data-bbox="1169 2035 1429 2202">  IRMA LUZ HERRERA RODRÍGUEZ Representante a la Cámara por Bogotá Partido Político MIRA </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 20px;"> <div data-bbox="876 2228 1104 2318">  MANUEL VIRGÚEZ PIRAQUIVE Senador de la República Partido Político MIRA </div> <div data-bbox="1169 2228 1429 2318">  CARLOS EDUARDO GUEVARA Senador de la República Partido Político MIRA </div> </div>

<p>RADICACIÓN DEL PROYECTO DE LEY "POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLÍTICA PÚBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS, Y ADOLESCENTES, SE MODIFICA LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES"</p> <p style="text-align: center;">SENADO DE LA REPÚBLICA Secretaría General (Art. 139 y ss Ley 5ª de 1.992)</p> <p>El día <u>12</u> del mes <u>Marzo</u> del año <u>2024</u> se radicó en este despacho el proyecto de ley N°. <u>254</u> Acto Legislativo N°. _____, con todos y cada uno de los requisitos constitucionales y legales por: <u>HS: Ana Paola Agudelo, Manuel Virguez</u> <u>Carlos Eduardo Guevara HR: Irma Luz Herrera</u></p> <p style="text-align: center;">SECRETARIO GENERAL</p>	<p style="text-align: center;">SECCIÓN DE LEYES</p> <p style="text-align: center;">SENADO DE LA REPÚBLICA – SECRETARÍA GENERAL – TRAMITACIÓN LEYES</p> <p>Bogotá D.C., 12 de marzo de 2024</p> <p>Señor Presidente:</p> <p>Con el fin de repartir el Proyecto de Ley No.254/24 Senado "POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLÍTICA PÚBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS Y ADOLESCENTES, SE MODIFICA LA LEY 1146 DE 2007, LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES", me permito remitir a su despacho el expediente de la mencionada iniciativa, presentada el día de hoy ante la Secretaría General del Senado de la República por los Honorables Senadores ANA PAOLA AGUDELO GARCÍA, MANUEL VIRGUEZ PIRAQUIVE, CARLOS EDUARDO GUEVARA VILLABON; y la Honorable Representante IRMA LUZ HERRERA RODRIGUEZ. La materia de que trata el mencionado Proyecto de Ley es competencia de la Comisión PRIMERA Constitucional Permanente del Senado de la República, de conformidad con las disposiciones Constitucionales y Legales.</p> <p>GREGORIO ELJACH PACHECO Secretario General</p> <p style="text-align: center;">PRESIDENCIA DEL H. SENADO DE LA REPÚBLICA – MARZO 12 DE 2024</p> <p>De conformidad con el informe de Secretaría General, dese por repartido el precitado Proyecto de Ley a la Comisión PRIMERA Constitucional y envíese copia del mismo a la Imprenta Nacional para que sea publicado en la Gaceta del Congreso.</p> <p>CÚMPLASE</p> <p>EL PRESIDENTE DEL HONORABLE SENADO DE LA REPÚBLICA</p> <p>IVÁN LEONIDAS NAME VÁSQUEZ</p> <p>SECRETARIO GENERAL DEL HONORABLE SENADO DE LA REPÚBLICA</p> <p>GREGORIO ELJACH PACHECO</p>
---	---

PONENCIAS

INFORME DE PONENCIA PARA SEGUNDO DEBATE AL PROYECTO DE LEY NÚMERO 59 DE 2023 SENADO

por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones.

<p>Honorable Senador IVÁN LEONIDAS NAME VÁSQUEZ Presidente Senado de la República</p> <p>Ref.: Informe de ponencia para segundo debate al Proyecto de Ley N° 059 de 2023 Senado "Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones".</p> <p>Estimado Presidente,</p> <p>En cumplimiento de la designación que me hiciera la Mesa Directiva de la Honorable Comisión Sexta Constitucional Permanente del Senado de la República, me permito rendir informe de ponencia positiva para segundo debate al Proyecto de Ley de la referencia bajo los siguientes términos:</p> <p>I. TRÁMITE DE LA INICIATIVA</p> <p>El proyecto fue radicado el 01 de agosto de 2.023 ante la Secretaría General del Senado de la República para surtir su trámite en la legislatura 2.023 – 2.024.</p> <p>En sesión del 14 de noviembre de 2023 fue aprobado el proyecto de ley en primer debate en la Comisión VI Constitucional del Senado de la República.</p> <p>Mediante oficio fechado 22 de noviembre de 2.023 de la mesa directiva de la Comisión VI Constitucional del Senado de la República, fui designado como ponente para segundo debate de esta iniciativa.</p> <p>Sus autores son los Honorables Senadores Juan Diego Echavarría Sánchez y Juan Carlos Garcés Rojas</p> <p>II. OBJETO DEL PROYECTO</p> <p>Esta iniciativa busca establecer lineamientos y principios orientadores en materia regulatoria y de política pública en todo aquello relacionado con el desarrollo e implementación de la Inteligencia Artificial.</p> <p>La apuesta principal del proyecto de ley es hacer de esta novedosa herramienta tecnológica un medio que esté al servicio del ser humano y del desarrollo social y económico sostenible y bajo claros criterios de seguridad, protección de datos y responsabilidad.</p> <p>III. MARCO LEGAL</p> <p>Para esta iniciativa han de tenerse en cuenta y consultarse las siguientes disposiciones de orden constitucional y legal.</p> <p>> CONSTITUCIONALES</p> <p>Artículos: 1, 2, 5, 6, 13, 14, 15, 16, 18, 19, 20, 21, 25, 26, 27, 28, 29, 44, 45, 58, 61, 67, 70,</p>	<p>71, 73, 74, 75, 78, 150 (No. 1, 7, 8, 23) 152, 154, 157 y 209, entre otras.</p> <p>> LEGALES</p> <p>Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"</p> <p>Ley 2162 de 2021 "Por medio de la cual se crea el Ministerio de Ciencia, Tecnología e Innovación y se dictan otras disposiciones"</p> <p>Ley 1955 de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022" (Art. 147)</p> <p>Ley 2294 de 2023 "Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida".</p> <p>> REGLAMENTARIAS U OTRAS</p> <p>CONPES 3975 "Política Nacional para la Transformación Digital e Inteligencia Artificial"</p> <p>IV. EXPOSICIÓN DE MOTIVOS</p> <p>A. JUSTIFICACIÓN</p> <p>Las iniciativas legislativas por medio de las cuales se establecen políticas públicas han sido desarrolladas en el ordenamiento jurídico colombiano. Ejemplo de éstas se encuentran la ley 1988 de 2019, por medio de la cual se establece la política pública para vendedores informales; la ley 1804 de 2016, por medio de la cual se establece la política de Estado para el Desarrollo Integral de la Primera Infancia de Cero a Siempre; la ley 1953 de 2019, por medio del cual se establece la política pública de prevención de la infertilidad; la ley 1641 de 2013, por medio de la cual se establece la política pública social para habitantes de la calle, entre otras.</p> <p>El derecho no es ajeno a las nuevas tecnologías. La implementación de TIC en ámbitos relacionados con la administración pública, comercio electrónico, servicios, open gov, inclusión, y otros más, conforme se aprecia al estudiar a Jairo Becerra¹, revisten una serie de escenarios en donde la IA se encuentra abriendo espacios en los cuales se desconoce el rumbo, y, por ende, de sus efectos positivos y negativos</p> <p>Así las cosas, y teniendo en cuenta que se considera necesario iniciar un proceso de regulación sobre la inteligencia artificial, un primer paso correspondería a la adopción de las políticas públicas frente a este tema.</p>
---	---

¹ BECERRA, JAIRO. [ET AL.]. El derecho y las tecnologías de la información y la comunicación (TIC) /. Bogotá: Universidad Católica de Colombia, 2015. Disponible en: <https://publicaciones.ucatolica.edu.co/pdf/el-derecho-y-las-tecnologias-de-la-informacion-y-la-comunicacion.pdf>

Alemania, conforme lo señala Rafael Torres Muñoz², se encuentra estableciendo políticas públicas para efectos de desarrollos en robótica e Inteligencia Artificial. Para dicho efecto ha iniciado avances en el uso de vehículos autónomos, la implementación de normas éticas en la IA. Adicionalmente, señala este autor que “no debe extrañar que, los países más avanzados en el desarrollo de tecnología robótica –Alemania en particular, creadora del concepto “Industria 4.0”, en el hemisferio occidental y Japón en el Oriental- sean pioneros en el desarrollo de políticas públicas basadas en investigación de vanguardia, que salvaguarden el derecho al trabajo, al bienestar y la seguridad de los seres humanos. En tanto que la Unión Europea y Estados Unidos de Norteamérica (EE.UU.) dada su conformación multiestatal, se encuentran aún en una fase de organización, definición de responsabilidades y coberturas.”.

Las políticas públicas adquieren vigencia en la implementación de la Inteligencia Artificial, puesto que se constituye en una herramienta que establece las reglas de aplicación y prevención, dados los efectos que se le ha atribuido a esta tecnología.

INTELIGENCIA ARTIFICIAL

La Real Academia Española³ ha definido a la inteligencia artificial como una “disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.”. Esta definición se adopta para los efectos del presente proyecto.

Uno de los primeros planteamientos es establecer la oportunidad de reglamentar la Inteligencia Artificial desde un marco jurídico. Algunos teóricos consideran que no es oportuno establecerla hasta que se cuente con un desarrollo generalizado de la misma; mientras que otros, como lo hace Elon Musk, conforme los recuerda Oren Etzioni⁴, señalan que debe hacerse antes de que sea demasiado tarde.

En el Foro Económico de Davos se abrió el espacio para determinar la necesidad de reglamentación de la Inteligencia Artificial. Allí se explicó que organismos internacionales trabajan en la materia por cuanto justifican que la necesidad de regular este tema se genera para obtener modelos confiables, conforme fue explicado por el periódico Portafolio⁵. Allí mismo, se hace evidente la posición que tienen importantes actores en el sector, como IBM Colombia, quien con la explicación que diera Catalina Rengifo, y quien es la responsable de Asuntos Gubernamentales para IBM, señalará que: “Una eventual regulación tendría muchas aplicaciones en el país, considerando que actualmente existe una alta implementación de la Inteligencia Artificial (IA) tanto en Colombia, como en el resto del mundo. Estamos frente a un tema vital. Los sistemas de Inteligencia Artificial deben ser transparentes y explicables, y debe haber un equilibrio entre la regulación y la autorregulación”⁶.

² TORRES, RAFAEL. Políticas Públicas para la Robótica y la Inteligencia Artificial. Biblioteca del Congreso Nacional de Chile. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26982/1/Políticas_Públicas_para_la_Robótica_y_la_Inteligencia_Artificial.pdf

³ REAL ACADEMIA ESPAÑOLA. Disponible en: <https://dle.rae.es/inteligencia%2Dmh%2C>

⁴ ETZIONI, OREN. ¿Cómo regular la inteligencia artificial? Septiembre 6 de 2017. The New York Times. Disponible en: <https://www.nytimes.com/es/2017/09/06/espanol/opinion/inteligencia-artificial-reglas-regulacion.html>

⁵ PORTAFOLIO. El país se alista ante la tarea de regular la inteligencia artificial. 31 de enero de 2020. Disponible en: <https://www.portafolio.co/tendencias/el-pais-se-alista-ante-la-tarea-de-regular-la-inteligencia-artificial-537664>

⁶ PORTAFOLIO. El país se alista ante la tarea de regular la inteligencia artificial. 31 de enero de 2020. Disponible en: <https://www.portafolio.co/tendencias/el-pais-se-alista-ante-la-tarea-de-regular-la-inteligencia-artificial-537664>

Frente al tema de la regulación y autorregulación, son varias las posiciones y más en una materia que se encuentra en constante desarrollo. Por ello se ha considera la improcedencia de establecer reglas fuertes que no coincidan a la par con los desarrollos tecnológicos e informáticos. Un ejemplo de ello son las propuestas que se han derivado en otros escenarios como el de las redes sociales a las cuales se les ha señalado ser parte de una responsabilidad social digital bajo un esquema de soft law⁷. Lo anterior, es importante resaltarlo para efectos de entender que este proyecto al soportarse en un enfoque de políticas públicas generales permitirá que los desarrollos de la IA tengan un objetivo político sin limitar sus procesos evolutivos.

Otro aspecto que sería objeto de análisis para verificar la regulación de la Inteligencia Artificial correspondería a los eventuales riesgos que la misma podría generar. Al respecto, Max Tegmark⁸, profesor de física e investigador de Inteligencia Artificial avizora una serie de peligros en la Inteligencia artificial, como el control por parte de unos sobre la misma y que su uso pueda ser impulsado en todo el planeta, a manera de ejemplo, un dictador, en donde las máquinas le obedecen.

Una reflexión importante sobre la inteligencia artificial es la que hace el profesor Max Tegmark⁹ cuando señala: “No debemos pensar en qué pasará, sino que debemos empezar preguntando qué es lo que queremos que pase.” Por ello se plantean, a manera de ejemplo, escenarios de análisis preventivos, como el que correspondería al desaparecimiento del empleos y profesiones.

Para María J. Santos G.¹⁰ debe existir una nueva regulación que preserve la autenticidad, seguridad y protección de la raza humana que involucren cuestiones éticas entendiendo que “[n]o se trata de regular la tecnología sino de regular la sociedad para que siga siendo para los humanos como ellos decidían.”.

La ley 1955¹¹ estableció en el art. 147 la transformación Digital Pública estableciendo en el numeral 6 la priorización de tecnologías emergentes de la cuarta revolución industrial teniendo como modelo la inteligencia artificial (AI). Sobre este mandato debe recordarse que Colombia además se adhirió a los acuerdos sobre Inteligencia Artificial por ser parte de los países de la Oede. Por este motivo, el gobierno nacional suscribió la recomendación del Consejo de la OCDE conforme lo manifestó el Ministerio de las TIC.¹²

⁷ ORTEGA, L. (2020). Facebook: derechos afectados y aspectos jurídicos de la red social. Revista Jurídicas, 17 (1), 165-186. DOI: 10.17151/revista.2020.17.1.9. Disponible en: [http://juridicas.ualdas.edu.co/downloads/Juridicas17\(1\)_9.pdf](http://juridicas.ualdas.edu.co/downloads/Juridicas17(1)_9.pdf)

⁸ REVISTA SEMANA. Inteligencia Artificial, ¿Oportunidad o amenaza? 24 de febrero de 2020. Disponible en: <https://www.semana.com/educacion/articulo/inteligencia-artificial-oportunidad-o-amenaza/653360>

⁹ PORTAFOLIO. Los peligros que traería la inteligencia artificial para la humanidad. 11 de febrero de 2020. Disponible en: <https://www.portafolio.co/tendencias/los-peligros-de-la-inteligencia-artificial-537654>

¹⁰ González, María José Santos. “Regulación legal de la robótica y la inteligencia artificial: retos de futuro- Legal regulation of robotics and artificial intelligence: future challenges.” Revista Jurídica de la Universidad de León 4 (2017): Pág. 28, 25-50. Disponible en: <http://revpubli.uileon.es/index.php/juridica/article/view/5285>

¹¹ REPUBLICA DE COLOMBIA, ley 1955 de 2019. DIARIO OFICIAL. AÑO CLV N. 50964, 25 MAYO DE 2019, PAG. 1. Disponible en: <http://www.sujin-jurisdic.gov.co/viewDocument.asp?ruta=Leves/30036488>

¹² REPUBLICA DE COLOMBIA, MINISTERIO DE LAS TIC, Colombia se adhiere a acuerdo sobre Inteligencias Artificial ante los países de la OCDE. Mayo 22 de 2019. Disponible en: <https://www.mintic.gov.co/portafolio/Sala-de-Prensa/Noticias/100683-Colombia-se-adhiere-a-acuerdo-sobre-Inteligencia-Artificial-ante-los-paises-de-la-OCDE>

La OCDE¹³ estableció recomendaciones para la implementación de la Inteligencia Artificial. Para ello ha establecido los siguientes principios:

Principio
Crecimiento inclusivo, desarrollo sostenible y bienestar.
Valores centrados en el ser humano y equidad
Transparencia y explicabilidad
Robustez, seguridad y protección.
Responsabilidad

Los principios expuestos fueron tenidos en cuenta en el articulado con el fin de implementarlos en el ordenamiento jurídico colombiano por medio de políticas públicas. A su vez, se tuvieron en cuenta las recomendaciones de la Oede¹⁴. A saber:

- Facilitar la inversión pública y privada en investigación y desarrollo para estimular la innovación en una IA confiable.
- Fomentar los ecosistemas de IA accesibles con infraestructura y tecnologías digitales y mecanismos para compartir datos y conocimientos.
- Asegurar un entorno de políticas que abra el camino para el despliegue de sistemas IA confiables.
- Capacitar a las personas con las habilidades para la IA y apoyar a los trabajadores para una transición justa.
- Cooperar a través de las fronteras y los sectores para avanzar en la administración responsable de IA confiable.

La dogmática de la inteligencia artificial ha usado en algunos escenarios el concepto de la persona electrónica, la cual fue estudiada en la presente investigación. Dicho escenario fue desvirtuado del presente proyecto por cuanto se consideró que generaba riesgos en cuanto a la imposibilidad de asignar responsabilidades por efectos de reparación de daños. Este asunto abrió la puerta para determinar si este concepto adquiriría una naturaleza jurídica diferente a las asignadas a la persona jurídica, o, por el contrario, debía tener una regulación especial dadas las semejanzas y diferencias que le atribuyen con ocasión de una inteligencia no humana.

Por ello, reconocerle vida jurídica a la persona electrónica implica una nueva categoría de sujeto de derechos que genera riesgos al desconocerse los efectos que pudieran generarse de las decisiones de IA. Asimilar la existencia jurídica de una persona electrónica implica a su vez, diseñar un esquema en donde igualmente se desarrollen escenarios jurídicos que diseñen los efectos por la muerte o desaparición de esta ficción. Así, por ejemplo, si la persona humana, al considerarse cadáver, aún es reconocida para efectos jurídicos como sujeto de responsabilidad jurídica por vía

¹³ ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS, OCDE. Recomendación del Consejo de Inteligencia Artificial. Adoptado el: 21/05/2019, Disponible en: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

¹⁴ República de Colombia, Ministerio de las TIC, Colombia se adhiere a acuerdo sobre Inteligencias Artificial ante los países de la OCDE. Mayo 22 de 2019. Disponible en: <https://www.mintic.gov.co/portafolio/Sala-de-Prensa/Noticias/100683-Colombia-se-adhiere-a-acuerdo-sobre-Inteligencia-Artificial-ante-los-paises-de-la-OCDE>

derechos y deberes, conforme lo recuerda Luis Germán Ortega Ruiz¹⁵ al señalar que “al cadáver humano [cuando] se le reconoce el principio de la dignidad, implica una protección al fuero moral y físico, desde el derecho al respeto, honra, buen nombre, un derecho al descanso eterno y esto se ha consolidado, por ejemplo, en los delitos del irrespeto a cadáveres, o la prohibición de despojo, el hurto de cadáveres y en conjunto con temas que ha revisado la Corte Constitucional; frente a las exhumaciones, es decir, el rito de sepultura, la última morada del cadáver etc.”.

Este aspecto es relevante para determinar si la persona electrónica podría considerarse como sujeto de derechos, y, a su vez, de obligaciones. Sobre este asunto, el proyecto de ley decidió no desarrollar esta figura bajo el ámbito de ser considerada como sujeto de derechos y deberes, trasladando la responsabilidad jurídica a los responsables en el uso, desarrollo e implementación de la inteligencia artificial, abarcando de esta manera, actores directos e indirectos bajo la categoría de persona jurídica o natural que tengan la capacidad jurídica de responder como sujeto de derecho y obligaciones.

La Inteligencia Artificial se encuentra en el orden del día de para su desarrollo constitucional en aras de establecer un marco teleológico que aspire a su uso para los fines esenciales del bien común. De allí que sea necesario recordar a Juan Francisco Sánchez Barrilao¹⁶ cuando explica que el derecho constitucional no puede negar la Inteligencia Artificial. Por tal razón expone posiciones como la de Esteve Pardo, Sánchez Barrilao, Muñoz Machado en las que enseña la posibilidad de adoptar conceptos jurídicos mutables con la tecnología. Ese escenario se plantea en este proyecto al adoptarse bajo los postulados de políticas públicas. Por otro lado, se señala como eje un enfoque apriorístico, el cual busca plantear anticipadamente escenarios generales que permitan a futura determinar los efectos por el uso e implementación de la IA en aras de evitar que ésta pueda ir en contravía de principios y derechos de protección constitucional.

Luis Germán Ortega Ruiz¹⁷ concluyó que “La implementación de la Inteligencia Artificial (IA) en el derecho es factible como medio o instrumento para la toma de decisiones jurídicas, pero no encuentra cabida como operador jurídico que reemplace la inteligencia humana para decidir en derecho aquellos casos del orden cualitativo. Lo anterior, sin perjuicio de poder usarse en materia de decisiones cuantitativas pero revisables por la inteligencia humana.”.

B. IMPACTO FISCAL

El artículo 7 de la Ley 819 de 2.003 establece que “el impacto fiscal de cualquier proyecto de ley, ordenanza o acuerdo, que ordene gasto o que otorgue beneficios tributarios, deberá hacerse explícito y deberá ser compatible con el Marco Fiscal de Mediano Plazo.”

¹⁵ ORTEGA-RUIZ, LUIS GERMÁN Y DUCUARA MOLINA, S. A. (2019). El cadáver humano y su incidencia jurídica. Revista Verba Iuris, 14 (42), pp. 73-98. Disponible en: <https://revistas.unillibe.edu.co/index.php/verbaluris/article/download/5680/5272>

¹⁶ BARRILAO, JUAN FRANCISCO SÁNCHEZ. “El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional.” Estudios de Deusto: revista de la Universidad de Deusto 64.2 (2016): 225-258. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=5878499>

¹⁷ ORTEGA-RUIZ, LUIS GERMÁN Y BECERRA, J. (2022) «La Inteligencia Artificial en la decisión jurídica y política», Araucaria, 24(49), doi: 10.12795.10. Disponible en: <https://revistascientificas.us.es/index.php/araucaria/article/view/15557>

Es importante resaltar que, la Honorable Corte Constitucional, mediante sentencia C-502 de 2007, consideró lo siguiente con respecto a la aplicación del artículo 7 de la Ley 819 de 2.003:

"Por todo lo anterior, la Corte considera que los primeros tres incisos del art. 7° de la Ley 819 de 2003 deben entenderse como parámetros de racionalidad de la actividad legislativa, y como una carga que le incumbe inicialmente al Ministerio de Hacienda, una vez que el Congreso ha valorado, con la información y las herramientas que tiene a su alcance, las incidencias fiscales de un determinado proyecto de ley. Esto significa que ellos constituyen instrumentos para mejorar la labor legislativa.

Es decir, el mencionado artículo debe interpretarse en el sentido de que su fin es obtener que las leyes que se dicten tengan en cuenta las realidades macroeconómicas, pero sin crear barreras insalvables en el ejercicio de la función legislativa ni crear un poder de veto legislativo en cabeza del Ministro de Hacienda.

Y en ese proceso de racionalidad legislativa la carga principal reposa en el Ministerio de Hacienda, que es el que cuenta con los datos, los equipos de funcionarios y la experiencia en materia económica. Por lo tanto, en el caso de que los congresistas tramiten un proyecto incorporando estimativos erróneos sobre el impacto fiscal, sobre la manera de atender esos nuevos gastos o sobre la compatibilidad del proyecto con el Marco Fiscal de Mediano Plazo, le corresponde al Ministro de Hacienda intervenir en el proceso legislativo para ilustrar al Congreso acerca de las consecuencias económicas del proyecto. Y el Congreso habrá de recibir y valorar el concepto emitido por el Ministerio. No obstante, la carga de demostrar y convencer a los congresistas acerca de la incompatibilidad de cierto proyecto con el Marco Fiscal de Mediano Plazo recae sobre el Ministro de Hacienda.

Por otra parte, es preciso reiterar que, si el Ministerio de Hacienda no participa en el curso del proyecto durante su formación en el Congreso de la República, mal puede ello significar que el proceso legislativo se encuentra viciado por no haber tenido en cuenta las condiciones establecidas en el art. 7° de la Ley 819 de 2003. Puesto que la carga principal en la presentación de las consecuencias fiscales de los proyectos reside en el Ministerio de Hacienda, la omisión del Ministerio en informar a los congresistas acerca de los problemas que presenta el proyecto no afecta la validez del proceso legislativo ni vicia la ley correspondiente."

Así las cosas, la interpretación constitucional conlleva a que la carga la asuma el Ministerio de Hacienda y Crédito Público con respecto a las iniciativas que pueden implicar gasto público y afectar el marco fiscal.

C. CONCLUSIÓN

Teniendo en cuenta las consideraciones expuestas, es necesario crear un marco jurídico en términos de reglamentación y como instrumento orientador de la política pública que impulse el desarrollo digital y tecnológico como herramienta útil al servicio del ser humano y el desarrollo social y económico sostenible.

Este proyecto reconoce una realidad imparable y que día a día, debido a su naturaleza dinámica, reta al país a acoger y adaptarse a un mundo absolutamente digitalizado en donde la tecnología transforma la vida y los paradigmas cotidianos.

V. IMPEDIMENTOS

Como ponente considero que difícilmente puede generarse un conflicto de interés en la participación legislativa de este proyecto por cuanto sus disposiciones son de carácter general y no están dirigidas a beneficiar, alterar, afectar, favorecer o perjudicar situaciones particulares y concretas.

Todo impedimento que se presente en el curso del trámite legislativo deberá tener la virtualidad de poner en evidencia la alteración o beneficio a favor o en contra del congresista o de sus parientes dentro de los grados previstos por la norma, de manera particular, actual y directa

VI. PROPOSICIÓN

Con base en las anteriores consideraciones, de manera atenta me permito presentar ponencia positiva, sin modificaciones, solicitándole a la plenaria del Senado de la República, dar segundo debate y aprobar el Proyecto de Ley No. 059 de 2023 Senado "Por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones".

Atentamente,

GUSTAVO ADOLFO MORENO HURTADO
Senador de la República

TEXTO PROPUESTO PARA SEGUNDO DEBATE EN SENADO

PROYECTO DE LEY N° 059 DE 2023 SENADO

"POR MEDIO DE LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE POLÍTICA PÚBLICA PARA EL DESARROLLO, USO E IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL Y SE DICTAN OTRAS DISPOSICIONES"

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO PRIMERO
DISPOSICIONES PRELIMINARES

ARTÍCULO 1. OBJETO. La presente ley tiene por objeto establecer los lineamientos de política pública para el desarrollo, uso e implementación de la Inteligencia Artificial.

ARTÍCULO 2. DEFINICIONES. Para efectos de interpretación de la presente ley se establecen las siguientes definiciones:

DATO: Información dispuesta para análisis y desarrollo de algoritmos.

INTELIGENCIA ARTIFICIAL: Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

ARTÍCULO 3. PRINCIPIOS. Para efectos de interpretación y aplicación de la presente ley se establecen los siguientes principios:

AUTORIDAD HUMANA: Toda decisión o dato de Inteligencia Artificial es auditable, revisable y controvertible por la decisión humana.

BIEN COMÚN: El uso, desarrollo e implementación de la Inteligencia Artificial no podrá tener como objetivo diferente el del bien común.

COOPERACIÓN: Las investigaciones en Inteligencia Artificial propenderán por la cooperación en materia de prevención del riesgo.

DISEÑO SEGURO: En todas las etapas de diseño y desarrollo de Inteligencia Artificial se deberán prever los efectos dañinos debiéndose abstener la implementación por evidencia de riesgo e inseguridad.

PREVALENCIA DE LA INTELIGENCIA HUMANA: Prevalecerá la decisión humana sobre los resultados que se establezca por medio de la Inteligencia Artificial.

INVESTIGACIÓN PREVENTIVA: Las investigaciones en inteligencia artificial en todo momento deberán contar con desarrollos paralelos de prevención de riesgos.

ARTÍCULO 4. COMISIÓN DE TRATAMIENTO DE DATOS Y DESARROLLOS CON INTELIGENCIA ARTIFICIAL. Créase una Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial, sin personería jurídica, que se conformará por:

- 1. El ministro de Ciencia, Tecnología e Innovación
2. El ministro de las Tecnologías de la Información y las Comunicaciones.
3. El Ministro de Educación Nacional
4. El Procurador General de la Nación
5. El director del Departamento Administrativo de Planeación Nacional.
6. Un representante de las universidades, el cual deberá contar con acreditación en alta calidad y acreditación institucional internacional.
7. La Superintendencia de Industria y Comercio
8. El Consejero Presidencial de Transformación Digital

ARTÍCULO 5. FUNCIONES DE LA COMISIÓN DE TRATAMIENTO DE DATOS Y DESARROLLOS CON INTELIGENCIA ARTIFICIAL. La Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial tendrá las siguientes funciones:

- 1. Avalar las solicitudes institucionales sobre desarrollos e implementación de Inteligencia Artificial.
2. Proyectar y divulgar los reglamentos técnicos para el uso, desarrollo e implementación de la Inteligencia Artificial.
3. Asesorar al Congreso de la República en las iniciativas relacionadas con Inteligencia Artificial.
4. Proponer iniciativas tecnológicas de Inteligencia Artificial en la gestión pública.
5. Proponer iniciativas tecnológicas de Inteligencia Artificial para el desarrollo económico, social y ambiental.
6. Evaluar el impacto de los desarrollos y su implementación con Inteligencia Artificial.
7. Darse su propio reglamento.

TÍTULO II
DE LA POLÍTICA SOBRE CRECIMIENTO INCLUSIVO, DESARROLLO SOSTENIBLE Y BIENESTAR

ARTÍCULO 6. INTELIGENCIA ARTIFICIAL PARA EL CRECIMIENTO INCLUSIVO. Las entidades del orden nacional y local que desarrollen políticas de crecimiento y productividad y que implementen la incorporación de Inteligencia Artificial deberán incluir frente a las metas de desarrollo económico, metas de desarrollo social.

ARTÍCULO 7. INTELIGENCIA ARTIFICIAL EN MATERIA DE CAMBIO CLIMÁTICO: El Gobierno Nacional por medio del Ministerio de Ambiente y Desarrollo Sostenible deberá reglamentar los requerimientos técnicos necesarios para implementar la inteligencia artificial en aras de

<p>la eficiencia energética, control de deforestación, movilidad amigable con el ambiente e incluirlo como instrumento de planificación y gestión conforme los términos de que trata la ley 1931 de 2018.</p> <p>ARTÍCULO 8. INTELIGENCIA ARTIFICIAL EN EL SISTEMA NACIONAL DE CAMBIO CLIMÁTICO: El Gobierno Nacional, por medio del Ministerio de Ambiente y Desarrollo Sostenible, incorporará en el Sistema Nacional de Cambio Climático la Inteligencia Artificial como instrumento para gestionar la mitigación de gases efecto invernadero y la adaptación al cambio climático.</p> <p style="text-align: center;">TÍTULO III DE LA POLITICA SOBRE LOS VALORES CENTRADOS EN EL SER HUMANO Y EQUIDAD</p> <p>ARTÍCULO 9. PREVALENCIA DE LA INTELIGENCIA HUMANA SOBRE LA INTELIGENCIA ARTIFICIAL. Las políticas del orden nacional o local para el uso, desarrollo e implementación de la inteligencia artificial deberán tener como propósito el bien común y la satisfacción de las necesidades propias del ser humano preservando en todo aspecto la prevalencia de la inteligencia humana sobre la inteligencia artificial.</p> <p>ARTÍCULO 10. PRESERVACIÓN DEL SER HUMANO Y SU ENTORNO AMBIENTAL. Las políticas del orden nacional o local para el uso, desarrollo e implementación de la inteligencia artificial deberán tener como propósito la preservación del ser humano y su entorno ambiental para la detección temprana de epidemias, diagnósticos de salubridad y desarrollo de medicamentos. Los desarrollos de Inteligencia Artificial podrán ser declarados de utilidad pública e interés social.</p> <p>ARTÍCULO 11. IGUALDAD EN EL DATO: Las políticas del orden nacional o local para el uso de los datos por parte de la Inteligencia Artificial no pueden permitir que se generen resultados que resulten como actos discriminatorios, por lo cual se deberá garantizar la igualdad de trato e igualdad de oportunidades.</p> <p>Parágrafo: La búsqueda de información por vía de Inteligencia Artificial que incida en restricciones de la libre competencia será sancionada por la Superintendencia de Industria y Comercio.</p> <p style="text-align: center;">TÍTULO IV DE LA POLITICA EN TRANSPARENCIA Y EXPLICABILIDAD</p> <p>ARTÍCULO 12. CONOCIMIENTO DEL USO DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial deberán garantizar la seguridad de la información respetando en todos los datos usados en el tratamiento que se les está otorgando a los mismos y los resultados obtenidos.</p>	<p>Parágrafo: Los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial deberán comunicar a los titulares de los datos que los mismos están interactuando con un sistema de IA y la manera en que lo está haciendo.</p> <p>Los titulares de los datos y sus herederos adquieren el derecho irrenunciable a eliminar el dato en cualquier momento. Para tal fin, los responsables que implementen y desarrollen Inteligencia Artificial deberán eliminar el dato dentro de los cinco (05) días hábiles siguientes a la solicitud de su titular.</p> <p>ARTÍCULO 13. COMPRESIÓN DEL USO DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial tienen la obligación de informar expresamente a los titulares el manejo que se les está dando a sus datos y los resultados obtenidos utilizando herramientas de comprensión especiales y atendiendo un nivel de inclusión conforme las características particulares de la persona y sus condiciones especiales.</p> <p>ARTÍCULO 14. EXPLICABILIDAD. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial tienen la obligación de garantizar que se conocen las causas que dan lugar a las decisiones, resultados o predicciones de los algoritmos obtenidos por la inteligencia humana.</p> <p style="text-align: center;">TÍTULO V DE LA POLITICA PARA LA ROBUSTEZ, SEGURIDAD Y PROTECCIÓN</p> <p>ARTÍCULO 15. DIRECCIÓN Y CONTROL. Las políticas del orden nacional o local deberán establecer que los sistemas de Inteligencia Artificial contarán con dirección, supervisión, auditoría y control de inteligencia humana capacitada y responsable.</p> <p>ARTÍCULO 16. CIBERSEGURIDAD. Las políticas del orden nacional o local deberán establecer que los asuntos de ciberseguridad que impliquen el uso, implementación y desarrollo de inteligencia artificial deberán ser avalados por la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial.</p> <p>ARTÍCULO 17. INSTRUMENTO DE SEGURIDAD NACIONAL. Las políticas del orden nacional o local deberán establecer que los asuntos que impliquen el uso, implementación y desarrollo de inteligencia artificial no podrán utilizarse como instrumento armamentista a menos que sea para asuntos de seguridad nacional.</p> <p>ARTÍCULO 18. DISEÑO SEGURO. Las políticas del orden nacional o local deberán establecer que el uso, implementación y desarrollo de Inteligencia Artificial deberá realizarse bajo el principio de diseño seguro, en el cual se deberán tener en cuenta efectos sociales, patrimoniales, laborales, económicos, ambientales, comerciales, políticos, y todos aquellos que tengan incidencia o generen riesgo en los seres humanos.</p> <p>ARTÍCULO 19. PRUEBA PREVIA. Las políticas del orden nacional o local deberán establecer que los responsables en el manejo de la Inteligencia Artificial deberán garantizar,</p>
<p>implementación de la Inteligencia Artificial, pruebas previas que garanticen la no generación de daños y la previsión de riesgos.</p> <p>ARTÍCULO 20. SEGURIDAD DE LA INFORMACIÓN: Las políticas del orden nacional o local deberán establecer que los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial deberán garantizar la seguridad de la información respetando en todo momento que no se vulnere el derecho a la intimidad y privacidad de las personas.</p> <p>ARTÍCULO 21. VERACIDAD DEL DATO Y DE LOS RESULTADOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial se vean obligados a realizar controles sobre la veracidad de los datos analizados y de los resultados que genere el sistema.</p> <p style="text-align: center;">TÍTULO VI DE LA POLITICA DE RESPONSABILIDAD</p> <p style="text-align: center;">CAPÍTULO I PROTECCIÓN DE DATOS</p> <p>ARTÍCULO 22. PROTECCIÓN DE DATOS GENERALES. Las políticas del orden nacional o local deberán establecer que los datos que sirvan para alimentar cualquier desarrollo de Inteligencia Artificial deberán contar con la autorización expresa de su titular y de los terceros que pudieran verse afectados.</p> <p>Parágrafo: La monetización de los datos usados por medio de inteligencia artificial cuyo beneficio se obtenga por el uso y análisis de la información suministrada por el titular de la información le permitirá a este exigir y reclamar, a manera de contraprestación, los réditos obtenidos sin su consentimiento más la indemnización de perjuicios.</p> <p>ARTÍCULO 23. PROTECCIÓN DE DATOS PERSONALÍSIMOS. Las políticas del orden nacional o local deberán establecer que los datos personalísimos como la voz, rasgos faciales, huellas digitales, ADN y otros que pertenezcan al cuerpo de un ser humano y que sirvan para alimentar cualquier desarrollo de Inteligencia Artificial deberá contar con la autorización expresa de su titular. Esta autorización deberá ser notificada al titular informando regularmente el uso de la información.</p> <p>Parágrafo: Le corresponde al responsable de la Inteligencia Artificial para la protección de datos personalísimos, renovar la autorización de que trata el presente artículo de manera trimestral.</p> <p>ARTÍCULO 24. RESERVA LEGAL. Las políticas del orden nacional o local deberán establecer que los datos generales y personalísimos usados en Inteligencia Artificial tienen reserva legal, por lo cual solamente podrán ser usados con autorización expresa de su titular.</p> <p>ARTÍCULO 25. USO DE DATOS PERSONALÍSIMOS. Las políticas del orden nacional o local deberán establecer que los datos personalísimos usados en Inteligencia Artificial no podrán ser usados con ánimo de lucro sin el consentimiento del titular de la información.</p>	<p>ARTÍCULO 26. EXCLUSIÓN DE DATOS. Las políticas del orden nacional o local deberán establecer que las personas titulares de datos que sean usados para efectos de desarrollos de Inteligencia Artificial podrán exigir la eliminación de sus datos en cualquier momento. Por lo anterior, el responsable del uso y manejo de la Inteligencia Artificial tendrá cinco (05) días para efectos de eliminar el dato y notificar a su titular su cumplimiento.</p> <p>ARTÍCULO 27. ANONIMIZACIÓN DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso de datos utilizados para la Inteligencia Artificial deberán garantizar la anonimización de la información de carácter particular.</p> <p style="text-align: center;">CAPÍTULO II RÉGIMEN DE RESPONSABILIDAD</p> <p>ARTÍCULO 28. RÉGIMEN DE RESPONSABILIDAD EXTRA CONTRACTUAL: Las políticas del orden nacional deberán establecer que los responsables en el uso, manejo e implementación de Inteligencia Artificial están sometidos al régimen de responsabilidad objetiva y deberán garantizar por medio de garantías la reparación de perjuicios materiales e inmateriales.</p> <p>ARTÍCULO 29. RÉGIMEN DE RESPONSABILIDAD CONTRACTUAL: Las políticas del orden nacional o local deberán establecer que las partes de un contrato estatal, en donde se haga uso de Inteligencia Artificial deberán pactar los riesgos que impliquen el uso frente a los eventuales daños o perjuicios que se generen como consecuencia de su implementación.</p> <p>ARTÍCULO 30. REGISTROS NACIONAL DE INTELIGENCIA ARTIFICIAL: Los desarrollos de Inteligencia Artificial deberán ser registrados ante el Ministerio de Ciencia, Tecnología e Innovación previo cumplimiento de los requisitos técnicos y jurídicos que para el efecto determine la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial.</p> <p>ARTÍCULO 31. CÓDIGO DE ÉTICA. Los responsables del uso, desarrollo e implementación de Inteligencia Artificial deberán radicar ante la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial un Código de Ética en el que se establezcan los responsables por los daños que se generen, garantizando el cumplimiento de la presente ley.</p> <p style="text-align: center;">TÍTULO VII DISPOSICIONES FINALES</p> <p>ARTÍCULO 32. VIGENCIA Y DEROGATORIA: La presente ley rige a partir de la fecha de su promulgación y deroga las disposiciones que le sean contrarias.</p>

Comisión Sexta Constitucional Permanente

TEXTO APROBADO EN PRIMER DEBATE POR LA COMISION SEXTA DEL SENADO DE LA REPUBLICA, EN SESION REALIZADA EL DIA 14 DE NOVIEMBRE DE 2023, DEL PROYECTO DE LEY No. 059 DE 2023 SENADO

"POR MEDIO DE LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE POLÍTICA PÚBLICA PARA EL DESARROLLO, USO E IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL Y SE DICTAN OTRAS DISPOSICIONES"

EL CONGRESO DE COLOMBIA

DECRETA:

TÍTULO PRIMERO
DISPOSICIONES PRELIMINARES

ARTÍCULO 1. OBJETO. La presente ley tiene por objeto establecer los lineamientos de política pública para el desarrollo, uso e implementación de la Inteligencia Artificial.

ARTÍCULO 2. DEFINICIONES. Para efectos de interpretación de la presente ley se establecen las siguientes definiciones:

DATO: Información dispuesta para análisis y desarrollo de algoritmos.

INTELIGENCIA ARTIFICIAL: Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

ARTÍCULO 3. PRINCIPIOS. Para efectos de interpretación y aplicación de la presente ley se establecen los siguientes principios:

AUTORIDAD HUMANA: Toda decisión o dato de Inteligencia Artificial es auditable, revisable y controvertible por la decisión humana.

BIEN COMÚN: El uso, desarrollo e implementación de la Inteligencia Artificial no podrá tener como objetivo diferente el del bien común.

COOPERACIÓN: Las investigaciones en Inteligencia Artificial propenderán por la cooperación en materia de prevención del riesgo.

DISEÑO SEGURO: En todas las etapas de diseño y desarrollo de Inteligencia Artificial se deberán prever los efectos dañinos debiéndose abstener la implementación por evidencia de riesgo e inseguridad.

PREVALENCIA DE LA INTELIGENCIA HUMANA: Prevalecerá la decisión humana sobre los resultados que se establezca por medio de la Inteligencia Artificial.

INVESTIGACIÓN PREVENTIVA: Las investigaciones en inteligencia artificial en todo momento deberán contar con desarrollos paralelos de prevención de riesgos.

ARTÍCULO 4. COMISIÓN DE TRATAMIENTO DE DATOS Y DESARROLLOS CON INTELIGENCIA ARTIFICIAL. Créase una Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial, sin personería jurídica, que se conformará por:

- 1. El ministro de Ciencia, Tecnología e Innovación
2. El ministro de las Tecnologías de la Información y las Comunicaciones.
3. El Ministro de Educación Nacional
4. El Procurador General de la Nación
5. El director del Departamento Administrativo de Planeación Nacional.
6. Un representante de las universidades, el cual deberá contar con acreditación en alta calidad y acreditación institucional internacional.
7. La Superintendencia de Industria y Comercio
8. El Consejero Presidencial de Transformación Digital

ARTÍCULO 5. FUNCIONES DE LA COMISIÓN DE TRATAMIENTO DE DATOS Y DESARROLLOS CON INTELIGENCIA ARTIFICIAL. La Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial tendrá las siguientes funciones:

- 1. Avalar las solicitudes institucionales sobre desarrollos e implementación de Inteligencia Artificial.
2. Proyectar y divulgar los reglamentos técnicos para el uso, desarrollo e implementación de la Inteligencia Artificial.
3. Asesorar al Congreso de la República en las iniciativas relacionadas con Inteligencia Artificial.
4. Proponer iniciativas tecnológicas de Inteligencia Artificial en la gestión pública.
5. Proponer iniciativas tecnológicas de Inteligencia Artificial para el desarrollo económico, social y ambiental.
6. Evaluar el impacto de los desarrollos y su implementación con Inteligencia Artificial.
7. Darse su propio reglamento.

TÍTULO II
DE LA POLITICA SOBRE CRECIMIENTO INCLUSIVO, DESARROLLO SOSTENIBLE Y BIENESTAR

ARTÍCULO 6. INTELIGENCIA ARTIFICIAL PARA EL CRECIMIENTO INCLUSIVO. Las entidades del orden nacional y local que desarrollen políticas de crecimiento y productividad y que implementen la incorporación de Inteligencia Artificial deberán incluir frente a las metas de desarrollo económico, metas de desarrollo social.

ARTÍCULO 7. INTELIGENCIA ARTIFICIAL EN MATERIA DE CAMBIO CLIMÁTICO: El Gobierno Nacional por medio del Ministerio de Ambiente y Desarrollo Sostenible deberá reglamentar los requerimientos técnicos necesarios para implementar la inteligencia artificial en aras de la eficiencia energética, control de deforestación, movilidad

amigable con el ambiente e incluirlo como instrumento de planificación y gestión conforme los términos de que trata la ley 1931 de 2018.

ARTÍCULO 8. INTELIGENCIA ARTIFICIAL EN EL SISTEMA NACIONAL DE CAMBIO CLIMÁTICO: El Gobierno Nacional, por medio del Ministerio de Ambiente y Desarrollo Sostenible, incorporará en el Sistema Nacional de Cambio Climático la Inteligencia Artificial como instrumento para gestionar la mitigación de gases efecto invernadero y la adaptación al cambio climático.

TÍTULO III
DE LA POLITICA SOBRE LOS VALORES CENTRADOS EN EL SER HUMANO Y EQUIDAD

ARTÍCULO 9. PREVALENCIA DE LA INTELIGENCIA HUMANA SOBRE LA INTELIGENCIA ARTIFICIAL. Las políticas del orden nacional o local para el uso, desarrollo e implementación de la inteligencia artificial deberán tener como propósito el bien común y la satisfacción de las necesidades propias del ser humano preservando en todo aspecto la prevalencia de la inteligencia humana sobre la inteligencia artificial.

ARTÍCULO 10. PRESERVACIÓN DEL SER HUMANO Y SU ENTORNO AMBIENTAL. Las políticas del orden nacional o local para el uso, desarrollo e implementación de la inteligencia artificial deberán tener como propósito la preservación del ser humano y su entorno ambiental para la detección temprana de epidemias, diagnósticos de salubridad y desarrollo de medicamentos. Los desarrollos de Inteligencia Artificial podrán ser declarados de utilidad pública e interés social.

ARTÍCULO 11. IGUALDAD EN EL DATO: Las políticas del orden nacional o local para el uso de los datos por parte de la Inteligencia Artificial no pueden permitir que se generen resultados que resulten como actos discriminatorios, por lo cual se deberá garantizar la igualdad de trato e igualdad de oportunidades.

Parágrafo: La búsqueda de información por vía de Inteligencia Artificial que incida en restricciones de la libre competencia será sancionada por la Superintendencia de Industria y Comercio.

TÍTULO IV
DE LA POLITICA EN TRANSPARENCIA Y EXPLICABILIDAD

ARTÍCULO 12. CONOCIMIENTO DEL USO DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial tengan la obligación de informar expresamente a los titulares de los datos usados en el tratamiento que se les está otorgando a los mismos y los resultados obtenidos.

Parágrafo: Los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial deberán comunicar a los titulares de los datos que los mismos están interactuando con un sistema de IA y la manera en que lo está haciendo.

Los titulares de los datos y sus herederos adquieren el derecho irrenunciable a eliminar el dato en cualquier momento. Para tal fin, los responsables que implementen y desarrollen Inteligencia Artificial deberán eliminar el dato dentro de los cinco (05) días hábiles siguientes a la solicitud de su titular.

ARTÍCULO 13. COMPRESIÓN DEL USO DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial tienen la obligación de informar expresamente a los titulares el manejo que se les está dando a sus datos y los resultados obtenidos utilizando herramientas de comprensión especiales y atendiendo un nivel de inclusión conforme las características particulares de la persona y sus condiciones especiales.

ARTÍCULO 14. EXPLICABILIDAD. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, implementación y desarrollo de la Inteligencia Artificial tienen la obligación de garantizar que se conocen las causas que dan lugar a las decisiones, resultados o predicciones de los algoritmos obtenidos por la inteligencia humana.

TÍTULO V
DE LA POLITICA PARA LA ROBUSTEZ, SEGURIDAD Y PROTECCIÓN

ARTÍCULO 15. DIRECCIÓN Y CONTROL. Las políticas del orden nacional o local deberán establecer que los sistemas de Inteligencia Artificial contarán con dirección, supervisión, auditoría y control de inteligencia humana capacitada y responsable.

ARTÍCULO 16. CIBERSEGURIDAD. Las políticas del orden nacional o local deberán establecer que los asuntos de ciberseguridad que impliquen el uso, implementación y desarrollo de inteligencia artificial deberán ser avalados por la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial.

ARTÍCULO 17. INSTRUMENTO DE SEGURIDAD NACIONAL. Las políticas del orden nacional o local deberán establecer que los asuntos que impliquen el uso, implementación y desarrollo de inteligencia artificial no podrán utilizarse como instrumento armamentista a menos que sea para asuntos de seguridad nacional.

ARTÍCULO 18. DISEÑO SEGURO. Las políticas del orden nacional o local deberán establecer que el uso, implementación y desarrollo de Inteligencia Artificial deberá realizarse bajo el principio de diseño seguro, en el cual se deberán tener en cuenta efectos sociales, patrimoniales, laborales, económicos, ambientales, comerciales, políticos, y todos aquellos que tengan incidencia o generen riesgo en los seres humanos.

ARTÍCULO 19. PRUEBA PREVIA. Las políticas del orden nacional o local deberán establecer que los responsables en el manejo de la Inteligencia Artificial deberán garantizar, previa implementación de la Inteligencia Artificial, pruebas previas que garanticen la no generación de daños y la previsión de riesgos.

ARTÍCULO 20. SEGURIDAD DE LA INFORMACIÓN: Las políticas del orden nacional o local deberán establecer que los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial deberán garantizar la seguridad de la información respetando en todo momento que no se vulnere el derecho a la intimidad y privacidad de las personas.

ARTÍCULO 21. VERACIDAD DEL DATO Y DE LOS RESULTADOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso, desarrollo e implementación de la Inteligencia Artificial se vean obligados a realizar controles sobre la veracidad de los datos analizados y de los resultados que genere el sistema.

TÍTULO VI
DE LA POLÍTICA DE RESPONSABILIDAD

CAPÍTULO I
PROTECCIÓN DE DATOS

ARTÍCULO 22. PROTECCIÓN DE DATOS GENERALES. Las políticas del orden nacional o local deberán establecer que los datos que sirvan para alimentar cualquier desarrollo de Inteligencia Artificial deberán contar con la autorización expresa de su titular y de los terceros que pudieran verse afectados.

Parágrafo: La monetización de los datos usados por medio de inteligencia artificial cuyo beneficio se obtenga por el uso y análisis de la información suministrada por el titular de la información le permitirá a este exigir y reclamar, a manera de contraprestación, los réditos obtenidos sin su consentimiento más la indemnización de perjuicios.

ARTÍCULO 23. PROTECCIÓN DE DATOS PERSONALÍSIMOS. Las políticas del orden nacional o local deberán establecer que los datos personalísimos como la voz, rasgos faciales, huellas digitales, ADN y otros que pertenezcan al cuerpo de un ser humano y que sirvan para alimentar cualquier desarrollo de Inteligencia Artificial deberá contar con la autorización expresa de su titular. Esta autorización deberá ser notificada al titular informando regularmente el uso de la información.

Parágrafo: Le corresponde al responsable de la Inteligencia Artificial para la protección de datos personalísimos, renovar la autorización de que trata el presente artículo de manera trimestral.

ARTÍCULO 24. RESERVA LEGAL. Las políticas del orden nacional o local deberán establecer que los datos generales y personalísimos usados en Inteligencia Artificial tienen reserva legal, por lo cual solamente podrán ser usados con autorización expresa de su titular.

ARTÍCULO 25. USO DE DATOS PERSONALÍSIMOS. Las políticas del orden nacional o local deberán establecer que los datos personalísimos usados en Inteligencia Artificial no podrán ser usados con ánimo de lucro sin el consentimiento del titular de la información.

ARTÍCULO 26. EXCLUSIÓN DE DATOS. Las políticas del orden nacional o local deberán establecer que las personas titulares de datos que sean usados para efectos de desarrollos de Inteligencia Artificial podrán exigir la eliminación de sus datos en cualquier momento. Por lo anterior, el responsable del uso y manejo de la Inteligencia Artificial tendrá cinco (05) días para efectos de eliminar el dato y notificar a su titular su cumplimiento.

ARTÍCULO 27. ANONIMIZACIÓN DE DATOS. Las políticas del orden nacional o local deberán establecer que los responsables en el uso de datos utilizados para la Inteligencia Artificial deberán garantizar la anonimización de la información de carácter particular.

CAPITULO II
RÉGIMEN DE RESPONSABILIDAD

ARTÍCULO 28. RÉGIMEN DE RESPONSABILIDAD EXTRA CONTRACTUAL: Las políticas del orden nacional deberán establecer que los responsables en el uso, manejo e implementación de Inteligencia Artificial están sometidos al régimen de responsabilidad objetiva y deberán garantizar por medio de garantías la reparación de perjuicios materiales e inmateriales.

ARTÍCULO 29. RÉGIMEN DE RESPONSABILIDAD CONTRACTUAL: Las políticas del orden nacional o local deberán establecer que las partes de un contrato estatal, en donde se haga uso de Inteligencia Artificial deberán pactar los riesgos que impliquen el uso frente a los eventuales daños o perjuicios que se generen como consecuencia de su implementación.

ARTÍCULO 30. REGISTROS NACIONAL DE INTELIGENCIA ARTIFICIAL: Los desarrollos de Inteligencia Artificial deberán ser registrados ante el Ministerio de Ciencia, Tecnología e Innovación previo cumplimiento de los requisitos técnicos y jurídicos que para el efecto determine la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial.

ARTÍCULO 31. CÓDIGO DE ÉTICA. Los responsables del uso, desarrollo e implementación de Inteligencia Artificial deberán radicar ante la Comisión de Tratamiento de Datos y Desarrollos con Inteligencia Artificial un Código de Ética en el que se establezcan los responsables por los daños que se generen, garantizando el cumplimiento de la presente ley.

TÍTULO VII
DISPOSICIONES FINALES

ARTÍCULO 32. VIGENCIA Y DEROGATORIA: La presente ley rige a partir de la fecha de su promulgación y deroga las disposiciones que le sean contrarias.

Comisión Sexta Constitucional Permanente

AUTO DE SUSTANCIACIÓN

En los términos anteriores, fue aprobado en Primer Debate por la Comisión Sexta, en sesión ordinaria realizada el día 14 de noviembre de 2023, el Proyecto de Ley No. 059 de 2023 SENADO "POR MEDIO DE LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE POLÍTICA PÚBLICA PARA EL DESARROLLO, USO E IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL Y SE DICTAN OTRAS DISPOSICIONES", según consta en el Acta No. 16, de la misma fecha.


JORGE ELIECER LAVERDE VARGAS
Secretario General
Comisión Sexta del Senado

Comisión Sexta Constitucional Permanente

AUTO DE SUSTANCIACIÓN

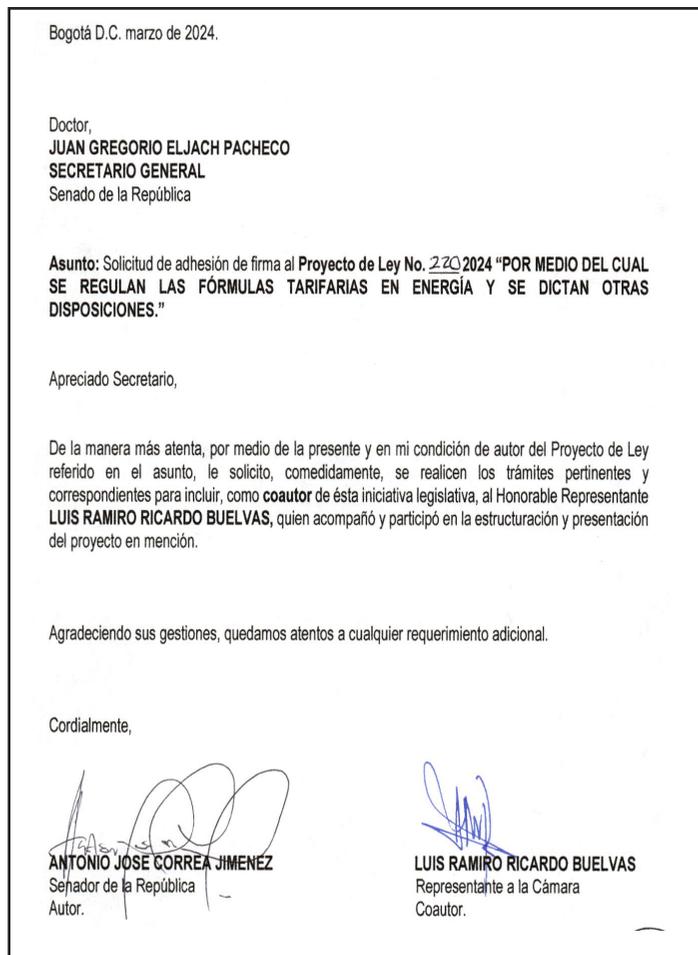
La Mesa Directiva Autoriza el Informe presentado para Segundo Debate por el Honorable Senador GUSTAVO ADOLFO MORENO HURTADO, al Proyecto de Ley No. 059 de 2023 SENADO "POR MEDIO DE LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE POLÍTICA PÚBLICA PARA EL DESARROLLO, USO E IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL Y SE DICTAN OTRAS DISPOSICIONES", DE ACUERDO AL ARTÍCULO 165 DE LA LEY 5ª DE 1992 "REGLAMENTO DEL CONGRESO", para que sea publicado en la Gaceta del Congreso.


JORGE ELIECER LAVERDE VARGAS
Secretario General
Comisión Sexta del Senado

CARTAS DE ADHESIÓN

CARTA DE ADHESIÓN AL PROYECTO DE LEY NÚMERO 220 DE 2024 SENADO HONORABLE SENADOR ANTONIO JOSÉ CORREA JIMÉNEZ Y HONORABLE REPRESENTANTE LUIS RAMIRO RICARDO BUELVAS

por medio del cual se regulan las fórmulas tarifarias en energía y se dictan otras disposiciones.



CONTENIDO

Gaceta número 233 - Miércoles, 13 de marzo de 2024	
SENADO DE LA REPÚBLICA	
PROYECTOS DE LEY	
Proyecto de ley número 254 de 2024 Senado, por medio de la cual se formulan lineamientos de política pública para la seguridad digital de niños, niñas y adolescentes, se modifica la Ley 1146 de 2007, la Ley 599 de 2000 y se dictan otras disposiciones.....	1

PONENCIAS

Informe de ponencia positiva para segundo debate, texto propuesto y texto aprobado al proyecto de ley número 59 de 2023 Senado, por medio de la cual se establecen los lineamientos de política pública para el desarrollo, uso e implementación de inteligencia artificial y se dictan otras disposiciones.....	7
CARTAS DE ADHESIÓN	
Carta de adhesión al proyecto de ley número 220 de 2024 Senado Honorable Senador Antonio José Correa Jiménez y honorable representante Luis Ramiro Ricardo Buelvas, por medio del cual se regulan las fórmulas tarifarias en energía y se dictan otras disposiciones.....	13