Bogotá D.C., 11 de abril de 2024

Honorable Senador
GERMÁN BLANCO ÁLVAREZ
Presidente
Comisión Primera Constitucional Permanente
Senado de la República
Ciudad

Asunto: Informe de ponencia para primer debate al 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"*.

Reciba un cordial saludo respetado señor Presidente,

En cumplimiento de la designación efectuada por la Mesa Directiva de la Comisión Primera Constitucional del Senado de la República y de acuerdo con lo establecido en el Artículo 156 de la Ley 5 de 1992, me permito rendir **informe de ponencia para primer debate al Proyecto de Ley No. 254 de 2024 Senad**o *"Por medio de la cual se formularan 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 "*, en los siguientes términos:

I. TRÁMITE DE LA INICIATIVA

El Proyecto de Ley bajo estudio fue radicado el 12 de marzo de 2024, ante la Secretaría General del Senado de la República. Es de autoría de los HH.SS. Ana Paola Agudelo García, Manuel Virguez Piraquive y Carlos Eduardo Guevara; y la H.R. Irma Luz Herrera Rodríguez. El texto original fue publicado en la Gaceta No. 233 de 2024.

El pasado 20 de marzo, mediante Acta MD-22, la Mesa Directiva de la Comisión Primera del Senado de la República designó como ponente única del Proyecto de Ley en mención a la H.S. Paloma Valencia Laserna.

II. OBJETO

El propósito de la presente iniciativa es establecer los lineamientos generales para la formulación e implementación de una política pública para la seguridad digital de los niños, niñas y adolescentes. Se busca que la política esté enfocada en la sensibilización, prevención y protección de menores de edad respecto a delitos realizados a través de internet, inteligencia artificial, redes sociales, medios informáticos y dispositivos móviles. También tiene como propósito la identificación, clasificación y tipificación de nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos contra niños, niñas y adolescentes y la población en general.

III. CONTENIDO DEL PROYECTO DE LEY

El texto de este Proyecto consta de 14 artículos dividido en tres capítulos, a saber:

El primer artículo dispone el objeto del proyecto de ley.

El primer capítulo, denominado Política Pública y sus Lineamientos, está conformado por los artículos 2 al 7, sobre los fines de la política pública, principios orientadores, lineamientos generales de la política pública, campañas y acciones pedagógicas de la política pública, acciones complementarias y el sistema de información sobre delitos sexuales contra menores.

El segundo capítulo, denominado Disposiciones Penales, está compuesto por los artículo 8 al 11, sobre un nuevo delito "difusión no consentida de imágenes con contenido sexual", un nuevo delito "acoso virtual a menores de edad", adición de

nuevos numerales de circunstancias de agravación en el artículo 245 de la Ley 599 de 2000 y bloqueos de usuarios y dominios de internet.

Y, el tercer capítulo, denominado Disposiciones Finales, está conformado por los artículos 12 a 14, sobre el Comité Interinstitucional Consultivo para la Prevención de la Violencia Sexual y Atención Integral de los Niños, Niñas y Adolescentes Víctimas del Abuso Sexual, adición de varios numerales al artículo 5 de la Ley 1146 de 2007 y vigencias y derogatorias.

IV. ANTECEDENTES DEL PROYECTO DE LEY

Para abordar los antecedentes de la presente iniciativa, se hará referencia directa a lo indicado en la exposición de motivos del Proyecto de Ley 254 de 2024. Como se señala en este texto, actualmente se cuenta el Acuerdo del Distrito 702 de 2018 "*por el cual se dictan lineamientos de política pública para la prevención, sensibilización y protección sobre crímenes cibernéticos contra niñas, niños y adolescentes de las Instituciones Educativas Distritales*". Este fue expedido por el Concejo de Bogotá, como producto del trabajo de la Bancada del Partido Político MIRA y de la colaboración de mesas de trabajo conjuntamente por la comunidad y la administración distrital desde el año 2015.

En la exposición, se indica que en el año 2016 la Bancada del Partido Político MIRA presentó en el Congreso de la República el Proyecto de Ley No. 050 de 2016 Cámara. En el marco de este proceso, recibió conceptos y recomendaciones del Consejo Superior de Política Criminal, Ministerio de Educación Nacional y el Instituto Colombiano de Bienestar Familiar.

Con base en ello, como explica en el texto, se radicó luego el Proyecto de Ley 74 de 2018 Senado "*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*", acumulado con el Proyecto de Ley 60 de 2018 Senado – 408 de 2019 Cámara, denominado "Proyecto de Seguridad Ciudadana".

También se recalcan como antecedentes de esta iniciativa los proyectos: (i) Proyecto de Ley No. 168 de 2020 Cámara "Por medio de la cual se tipifica el delito de violencia sexual cibernética, y se dictan otras disposiciones", cuyo autor es H.S. Richard Aguilar y (ii) Proyecto de Ley No. 147 de 2023 Cámara "Por medio de la cual se modifica el código penal, se establece el tipo penal de ciberacoso sexual de menores y se dictan otras disposiciones", cuyos autores son H.S. Nicolás Albeiro Echeverri Alvarán y H.R. Andrés Felipe Jiménez Vargas.

Sobre el marco normativo actual de la materia, la exposición de motivos señala que se tienen las siguientes normas: (i) 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; (ii) artículo 56 de la Ley 1450 de 2011, el cual regula el principio de neutralidad en la Red; (iii) Ley 1336 de 2009, la cual trata dispone un articulado de lucha contra la explotación, pornografía y turismo sexual con menores; y (iv) Ley 1273 de 2009, la cual modifica el Código Penal y crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos", el cual consagró varias modalidades ciber delictuales.

V. CONTEXTO

Este apartado se remitirá a lo indicado en la exposición de motivos de la iniciativa objeto de esta ponencia. Se señala que la masificación de las tecnologías de la información y de la comunicación ha permitido la participación mayoritaria de la ciudadanía en espacios virtuales. Esto en ejercicio de derechos de suma relevancia, como el acceso a la información pública, el habeas data y la intimidad. Se explica que esto conlleva a que, en la actualidad, el Estado tenga el deber de garantizar la convivencia pacífica de los ciudadanos tanto en el territorio nacional, como en los espacios virtuales que estén bajo su control. Resaltan que dicho deber de protección adquiere especial relevancia, si se tiene en cuenta que el proceso de renovación tecnológica también ha implicado un avance sin igual en materia de criminalidad.

Se enfatiza que algunos de los elementos que han incentivado el uso de tecnologías de la información y de las comunicaciones por parte de los delincuentes para cometer conductas punibles son las siguientes: (i) la posibilidad de intercambiar información con otras personas sin una identificación real, (ii) las dificultades en

materia de investigación y judicialización para determinar quién utilizó el mecanismo electrónico, (iii) la facilidad para alterar la evidencia, (iv) el carácter transnacional de las conductas, (v) la escasa conciencia de los usuarios sobre la necesidad de mantener unas mínimas medidas preventivas de seguridad y (vi) los bajos costos y riesgos que implican este tipo de operaciones.

En la exposición de motivos se aclara que el Proyecto de Ley regula delitos cometidos contra menores de edad. Y, en adición a ello, otorga nuevas herramientas a la Fiscalía, con el objeto de facilitar la investigación y judicialización de estos delitos.

VI. IMPACTO ACTUAL DE CRÍMENES CIBERNÉTICOS EN EL MUNDO

Haciendo referencia a lo indicado en la exposición de sobre el panorama global del bullying y ciberbullying, se tiene que, según el último estudio adelantado por la ONG Internacional Bullying Sin Fronteras entre enero de 2022 y abril de 2023, la situación en esta materia es alarmante y creciente. El fin de dicho estudio es arrojar luz sobre la magnitud de este problema en todo el mundo, con ayuda de miles de estudiantes, profesores de prestigiosas universidades y la cooperación de hospitales y ministerios de educación.

Se indica que los resultados del estudio son impactantes. Este describe el bullying y el ciberbullying como "asesinos silenciosos" que cada año son responsables de la muerte de 200,000 niños y jóvenes en todo el mundo. Dichos actos se alimentan de tres venenos: la soledad, la tristeza y el miedo, lo cual perpetúa un ciclo de sufrimiento entre las víctimas.

Se señala que este informe determina que México es el país con la mayor cantidad de casos registrados, con 270,000 incidentes graves de bullying y ciberbullying. Estas cifras representan un crecimiento del 50% respecto al informe previo, lo cual coloca a México en primer lugar a nivel mundial, seguido por Estados Unidos y España, con un gran número de incidentes.

La exposición de motivos recalca que el estudio busca actuar como un llamado de atención para combatir estos problemas, y no solo informar sobre la gravedad y

prevalencia del bullying y ciberbulying en el mundo. Y, aclara que reconocer y visibilizar el bullying como un problema global urgente es un paso elemental para desarrollar estrategias efectivas de prevención y apoyo a las víctimas[1].

Se señala que, según la UNICEF, uno de cada cinco jóvenes dejaron de asistir al colegio debido a que sufrían algún tipo de acoso en línea[2]. Explican que en América Latina siete de cada diez niños y adolescentes son víctimas de ciberacoso. De igual forma, el estudio concluyó que el 71% de los encuestados consideran que el acoso en Internet se da principalmente en las redes sociales.

La exposición hace referencia a un examen realizado por la INTERPOL en el 2018. Indica que este concluye que "*cuanto más joven era la víctima, más grave era el abuso; el 84% de las imágenes contenía actividad sexual explícita; más del 60% de las víctimas no identificadas eran prepubescentes, inclusive bebés y niños pequeños*"[3]. Se señala que la Sociedad para la Prevención de la Crueldad de los Niños sostiene que, desde la llegada del Coronavirus, los casos de '*online child abuse*' han incrementado exponencialmente. Además, indican que tan solo en el Reino Unido hay más de 25,300 niños víctimas de ciber delitos y que 90 niños son víctimas cada día[4].

Se hace referencia a un estudio adelantado por la Fundación ANAR y Fundación Mutua Madrileña, en España, el cual recoge la opinión de 10.901 estudiantes y 491 docentes entre enero de 2020 y junio de 2021. Este concluye que el ciberbullying es la forma de acoso que ha estado más presente desde que comenzó la pandemia, ya que una cuarta parte de los alumnos afirma conocer compañeros de clase que podrán haberlo sufrido. También concluye que ya no solo se produce a través de WhatsApp (53,9% de los casos), sino también a través de Instagram (44,4%), TikTok (38,5%) o videojuegos (37,7%). Se indica que los motivos más frecuentes por los que se producen estas agresiones son el aspecto físico (52,5%), por ser diferente (46,4%),

[1] Bullying Sin Fronteras (s.f.). *Bullying Sin Fronteras.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://bullyingsinfronteras.blogspot.com/2023/09/estadisticas-mundiales-de-bullying.html

[2] UNICEF (2020). *UNICEF busca empoderar a jóvenes para evitar el acoso y prevenir los riesgos en línea*. Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.unicef.org/colombia/comunicados-prensa/unicef-busca-empoderar-a-jovenes-para-evitar-el-acoso-y-prevenir-los-riesgos-en-linea#:~:text=U%20Report%20destaca%20que%201,en%20estado%20de%20ansiedad%20constante

[3] INTERPOL (s.f.). *Base de Datos Internacional sobre Explotación Sexual de Niños.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Base-de-Datos-Internacional-sobre-Explotacion-Sexual-de-Ninos

[4] The Guardian (2020). *Coronavirus lockdown raises risk of online child abuse, charity says*. Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.theguardian.com/world/2020/apr/02/coronavirus-lockdown-raises-risk-of-online-child-abuse-charity-says

por las cosas que hace o dice (39,1%), por sus gustos (30,4%), por ser de otro país, cultura, raza o religión (26,2%), por ser nuevo (20,1%), por su orientación sexual (15,2%) o por tener mucho o poco dinero (14,2%)[5].

Por otro lado, se recalca que en 2018, en España se llegó a la siguiente conclusión: "*actualmente, la importancia de la cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Pero otro hecho innegable es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad. (...) hemos pasado del año 2011, donde nos situábamos en el 2,1% al año 2018 con el 7,0%"*[6].

En la exposición de motivos se resalta el estudio de Evaluación de la Amenaza Global[7] realizado en 2021 por We Protect Global Alliance. Este encontró que la explotación y el abuso sexual infantil se sigue proliferando. De igual forma, indica que muchas de las 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. Y, sobre el ciberacoso, señala 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. Además, hay más de 3.000.000 de cuentas registradas en las 10 páginas más dañinas sobre abuso sexual infantil de la Dark Web. En promedio, 30 analistas del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) procesan 60.000 denuncias diarias en línea de abuso sexual infantil a través de CyberTipline.

En este estudio también se encontraron los siguientes datos relevantes. 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

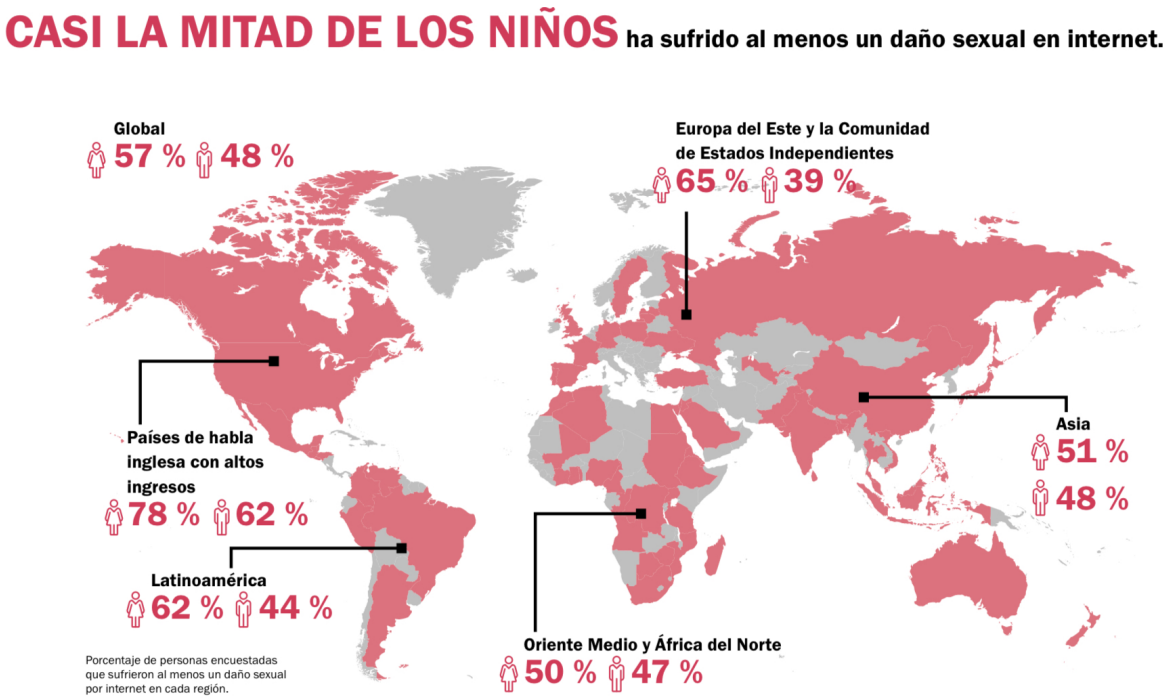
[5] RTVE (2021). *El ciberacoso aumenta entre los escolares desde el inicio de la pandemia y las agresiones grupales suben un 65%.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.rtve.es/noticias/20210915/acoso-escolar-agresiones-grupales-pandemia/2171018.shtml

[6] Ministerio del Interior – Gobierno de España. *Informe sobre la Cibercriminalidad en España.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

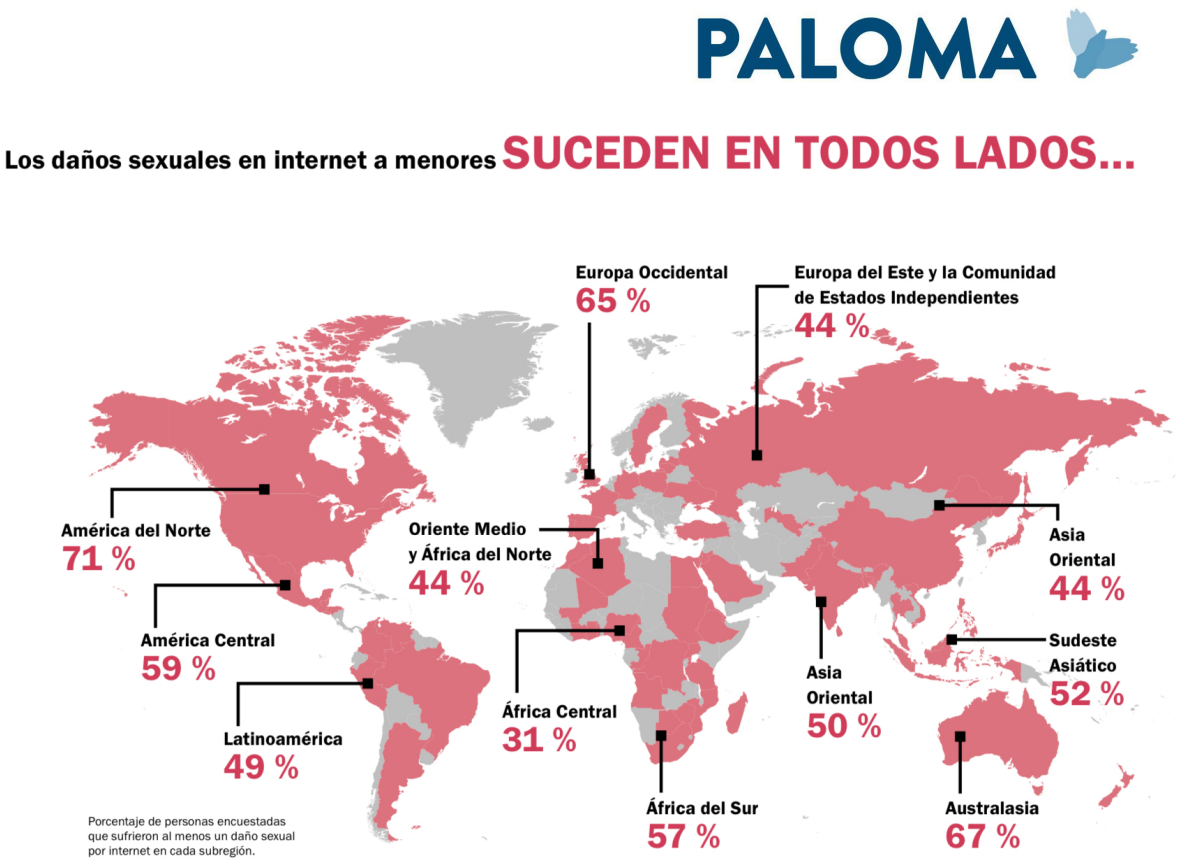
[7] We Protect Global Alliance (2021). *Evaluación de la Amenaza Global de 2021.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021-Report_Spanish.pdf

línea y el 29% afirmó que alguien compartió imágenes o videos sexualmente explícitos de los menores sin permiso.

Con esto, la exposición de motivos incluye las siguientes gráficas, en las cuales se detalla el porcentaje a nivel global de niños que sufren daños sexuales en internet (gráfica 1) y el porcentaje de los daños sexuales a menores por continente (gráfica 2).



Gráfica 1. We Protect Global Alliance (citada por la Exposición de Motivos del Proyecto de Ley No. 254 de 2024).



Gráfica 2. We Protect Global Alliance (citada por la Exposición de Motivos del Proyecto de Ley No. 254 de 2024).

Por otro lado, se señala que la EUROPOL sostiene 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]. De igual forma, se cita lo que la EUROPOL indica en el Internet Organised Crime Threat Assessment (IOCTA) 2023[9]. Explica que este 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. También indica que este informe sirve como una llamada de atención para individuos, empresas y gobiernos sobre la creciente sofisticación y alcance de las actividades ilícitas en línea.

[8] EUROPOL (s.f.). *Child Sexual Exploitation.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

[9] EUROPOL (2023). *Internet Organised Threat Assessment (IOCTA).* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

La exposición recalca que uno de los hallazgos más alarmantes se refiere a la escalada de ciberataques políticamente motivados, particularmente en el marco de la invasión de Ucrania por Rusia. Indica que dichos ataques 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 geopolítca como un nuevo campo de batalla en el ciber espacio. Esto además de revelar las divisiones políticas dentro de la comunidad cibercriminal.

Se explica que 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 sitios web falsos y campañas de recaudación de fondos fraudulentas. El documento afirma que este oportunismo subraya la naturaleza depredadora de los ciberdelincuentes, quienes están listos para explotar las tragedias humanitarias para su propio beneficio.

La exposición sostiene que, 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. Explica que este crimen destaca la necesidad de una vigilancia constante y la cooperación internacional para proteger a los más vulnerables de nuestra sociedad.

Se indica que el informe trata la compleja red de servicios de cibercrimen. Esto 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. Señala que la interconexión de estos servicios muestra un ecosistema criminal bien organizado y altamente especializado, lo cual plantea desafíos significativos para su detección y desmantelamiento.

Por otro lado, la exposición resalta que 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. Afirma que 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.

Se indica que la victimización múltiple es un tema recurrente, con individuos y organizaciones enfrentando ataques sucesivos o simultáneos. Asevera que esto 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.

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

Finalmente, indica que el informe 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. Esto no solo refuerza 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.

Por otro lado, la exposición hace referencia al Informe Anual 2022[10] de la INTERPOL, la cual ofrece una perspectiva detallada y alarmante sobre la ciberdelincuencia a nivel global, enfatizando los delitos cometidos contra menores de edad en el ciberespacio. Señala que este documento, producto 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.

Se indica que el informe encontró un aumento significativo en la cantidad y gravedad de los delitos cibernéticos, con especial atención a los dirigidos contra menores. Además, recalca que la Base de Datos Internacional de INTERPOL sobre

[10] INTERPOL (2022). *Informe Anual 2022*. Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://www.interpol.int/es/content/download/19843/file/INTERPOL%20%20Annual%20Report%202022_SP.pdf

Explotación Sexual de Niños (ICSE) ha permitido la identificación de 32,700 víctimas y 14,500 delincuentes, con una media de 7 víctimas identificadas cada día. De igual forma, la INTERPOL ha realizado operaciones significativas contra la ciberdelincuencia. Estas han incluido la coordinación de esfuerzos contra la ciberdelincuencia en 27 países de África, lo cual ha resultado en la detención de 11 personas y la acción contra más de 200,000 fragmentos de infraestructuras de malware.

Se afirma que 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. Señala que una operación policial internacional, apoyada por la INTERPOL, desmanteló una red transnacional dedicada a la extorsión sexual, resultando en la detención de 12 sospechosos principales. Con esto, concluye que 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.

Se destaca que el informe subraya la necesidad de una acción coordinada y decidida por parte de las autoridades globales, la industria tecnológica y las organizaciones de la sociedad civil para combatir estos hechos. Y, 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.

Por último, en la exposición de motivos se señala que la 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. Además, que 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.

VII. IMPACTO ACTUAL DE CRÍMENES CIBERNÉTICOS EN COLOMBIA

En esta sección de la ponencia se hará referencia a las explicaciones abordadas por la exposición de motivos respecto al impacto actual de crímenes cibernéticos en Colombia. En primer lugar, se indica que, según cifras de 2021 y procesos investigativos desarrollados por el Centro Cibernético Policial[11], las aplicaciones de mayor uso para la distribución de Material de Abuso Sexual Infantil son Whatsapp, Telegram, Facebook, Snapchat e Instagram.

También se hace referencia al Balance de Ciberseguridad 2023[12], el cual 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. Y, con esto, indica que las principales cifras y hechos destacados del documento son los siguientes.

Por un lado, afirma que 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. Explica que algunas de las modalidades de delitos informáticos más destacadas, son (i) el phishing, con 6,804 incidentes, evidenciando una disminución del 12% en comparación con el año anterior, y (ii) las estafas relacionadas con la compra y/o venta de productos en internet, que registraron 2,035 incidentes, mostrando una disminución significativa del 64%.

Además, recalca que el documento pone de relieve la falsedad personal en entornos digitales y las amenazas a través de redes sociales. Esto con 875 y 806 incidentes respectivamente, marcando una disminución del 16% en ambos casos. Indica que estas cifras subrayan la importancia de la prevención y la educación en materia de seguridad cibernética para mitigar los riesgos asociados a estas actividades delictivas.

---

[11] Centro de Capacidades para la Ciberseguridad de Colombia (2021). *Materia de Abuso Sexual Infantil (MASI).* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://drive.google.com/file/d/1JqXb5Avf0-vsKhSfA7zfYCwk-WFT2CBU/view

[12] Dirección de Investigación Criminal e INTERPOL – Centro Cibernético Policial (2023). *Balance de Ciberseguridad 2023.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

Por otro lado, asevera que la implementación de la segunda versión del CAI Virtual, el 22 de febrero de 2023, constituye un hito importante en la lucha contra la ciberdelincuencia. Se explica que esta plataforma, pionera en Iberoamérica, se dedica a la prevención, sensibilización y atención de incidentes cibernéticos, ofreciendo un servicio en línea disponible 24/7 para la ciudadanía. Y, recalca que esta iniciativa refleja el compromiso y la adaptación a las nuevas demandas de seguridad en el ciberespacio, proporcionando un recurso valioso para la protección contra los delitos informáticos[13].

Ahora bien, concretamente sobre Bogotá, la exposición de motivos indica que, según la Cámara Colombiana de Informática y Telecomunicaciones, la ciudad registró un 28.4% de los delitos cibernéticos del país en 2022. Además, indica que en la capital se reportó un total de 15.411 denuncias por este tipo de delitos, lo que representa un 28.4% del total de casos a nivel nacional.

Señala que según las cifras entregadas por el Centro Cibernético de la Policía, Bogotá es la ciudad del país con mayor reporte de ciberdelitos con 7.359 denuncias, lo que representa el 31% de las cifras. En segundo lugar se encuentra Medellín, con el 8% de los casos del país (1.910). Por su lado, todo el departamento de Cundinamarca ha denunciado 1.772 ciberdelitos, lo que equivale al 7.5% de los reportes.

Explica que, en virtud de las cifras anteriores y dando cumplimiento al Acuerdo Distrital 702 de 2018 *"por el cual se dictan lineamientos de política pública para la prevención, sensibilización y protección sobre crímenes cibernéticos contra niñas, niños, y adolescentes de las Instituciones Educativas Distritales*", la Alcaldía Mayor de Bogotá lanzó en 2023 "Alerta en línea". Esta es una estrategia para prevenir "ciberdelitos" que afectan a jóvenes en Bogotá, involucrando a estudiantes, docentes, padres de familia, la Secretaría de Seguridad y la empresa de telefonía móvil WOM Colombia y la Policía, con el acompañamiento de la Secretaría de Educación[14]. E indica que la estrategia tuvo como fin reforzar la prevención de ciberdelitos tal como el "Grooming", el "Sexting" y el ciberacoso con la formación de estudiantes, docentes y padres de familia.

---

[13] Idem.

[14] Alcaldía Mayor de Bogotá (2023). *Boletín de Prensa: "Alerta en Línea", la nueva estrategia para prevenir 'ciberdelitos' que afectan a jóvenes en Bogotá.* Citado en la Exposición de Motivos del Proyecto de Ley No. 254 de 2024. Recuperado de: https://scj.gov.co/sites/default/files/archivos-adjuntos/Alerta%20en%20l%C3%ADnea%2C%20la%20nueva%20estrategia%20para%20prevenir%20%E2%80%98ciberdelitos%E2%80%99%20que%20afectan%20a%20j%C3%B3venes%20en%20Bogot%C3%A1.pdf

VIII. EXPLICACIÓN DEL ARTICULADO

En este apartado se hará referencia directa a las explicaciones del articulado incluidas en la exposición de motivos del Proyecto de Ley No. 254 de 2024:

- Artículo 1: *"(…) consagra el objeto de la ley, estableciendo los lineamientos generales para la formulación e implementación de una política pública para la seguridad digital de los niños, niñas y adolescentes. Esta política se enfocará en la sensibilización, prevención y protección de este grupo frente a delitos cometidos a través de internet, inteligencia artificial, redes sociales, medios informáticos y dispositivos móviles. Además, busca identificar, clasificar y tipificar nuevas acciones criminales ejecutadas en el ciberespacio como delitos cibernéticos"*[15].

- Artículo 2: *"(…) se centra en los fines de la política pública propuesta por la ley. Los fines incluyen la sensibilización sobre los riesgos en el entorno digital, la prevención de delitos informáticos contra menores, y la protección de su integridad física y mental. También destaca la importancia de facilitar el restablecimiento de los derechos de los menores afectados por tales delitos"*[16].

- Artículo 3: *"(…) destaca los principios orientadores de la política pública. Estos principios incluyen la prevención de delitos cibernéticos, la pertinencia de las medidas adoptadas a los nuevos contextos tecnológicos, la coordinación entre diferentes niveles de la administración pública, y la articulación de esfuerzos entre los diversos actores involucrados en la protección de menores"*[17].

- Artículo 4: *"(…) se centra en los lineamientos generales para la formulación de la política pública. Asigna responsabilidades al Ministerio de Tecnologías de la Información y las Comunicaciones, en colaboración con la Fiscalía General de la Nación, el Instituto Colombiano de Bienestar Familiar, y otras entidades*

[15] Exposición de Motivos del 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"*. Gaceta 233 de 2024.
[16] Idem.
[17] Idem.

competentes, para caracterizar las prácticas y delitos más comunes contra menores en el ámbito digital y fortalecer los mecanismos de denuncia e información"[18].

- Artículo 5: *"(…) trata sobre las campañas y acciones pedagógicas que deben llevarse a cabo para promover un uso seguro y responsable de las TIC entre menores, padres de familia, educadores, y otros actores relevantes. Incluye la sensibilización sobre los riesgos en el entorno digital y la promoción de prácticas de seguridad informática"*[19].

- Artículo 6: *"(…) instruye al Ministerio de Educación Nacional a desarrollar guías para que las instituciones educativas puedan implementar programas de formación dirigidos a la identificación y denuncia de delitos informáticos contra menores. También promueve la creación de herramientas pedagógicas e informáticas que contribuyan a la protección de los menores en el entorno digital"*[20].

- Artículo 7: *"(…) modifica el artículo 15° de la Ley 679 de 2001. Propone la creación de un sistema de información para la prevención de delitos sexuales contra menores de edad y el control sobre quienes los cometan, promuevan o faciliten. Este sistema contará con una base de datos completa sobre delitos contra la libertad, el pudor y la formación sexual cometidos sobre niños, niñas y adolescentes y aquellos que se cometan a través de medios informáticos o electrónicos contra menores de 18 años, sus autores, cómplices, proxenetas, tanto de condenados. Además, promueve 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"*[21].

- Artículo 8: *"(…) crea el delito de Sexting, consiste en realizar alguna de estas conductas:*

    a. *Publicar, divulgar o revelar, imágenes o grabaciones audiovisuales de la actividad sexual o con contenido sexual de una persona, sin su autorización, en redes de información o comunicación;*

[18] Idem.
[19] Idem.
[20] Idem.
[21] Idem.

b. Ofrecer o entregar a un tercero las imágenes o las grabaciones audiovisuales de la actividad sexual o con contenido sexual de una persona, sin su consentimiento, a un tercero.

La finalidad principal de este delito pluriofensivo es la protección a la integridad e intimidad sexual de las personas. Sin embargo, su creación también permitirá la salvaguarda de la autonomía personal, en tanto que sanciona el constreñimiento a realizar conductas a cambio de evitar la publicación, o divulgación de las imágenes, o grabaciones de la actividad sexual, o con contenido sexual de las personas, esta situación no está contemplada en el ordenamiento legal vigente y para castigarla hay que hacer un salto a muchos tipos penales, esta situación dificulta la persecución criminal.

Como se observa, se trata de conductas que hoy en día no están punidas por otro tipo penal. Por su parte, como medida para robustecer la respuesta integral a las afectaciones que sufren las personas en su intimidad sexual, la iniciativa propone la inclusión de un agravante en el delito de extorsión, para aquellos casos en los que la amenaza de publicar, divulgar o revelar, a través de cualquier medio o red de información o de comunicación, imágenes o grabaciones audiovisuales de actividades sexuales o con contenido sexual, pretenda la obtención de un beneficio económico. Es decir, para aquellos casos en que las personas sean extorsionadas para evitar la divulgación de imágenes o grabaciones audiovisuales relacionadas con su intimidad sexual.

Actualmente, la jurisprudencia ha optado en algunos casos, por señalar que este tipo de conductas constituye una injuria por vía de hecho, en otros, un acto sexual. No obstante, el hecho que se haya optado por esas formas no convencionales para no desproteger a las personas no implica que esa sea la solución jurídica correcta. En efecto, debe regularse y debe regularse con un bien jurídico sustancialmente distinto al protegido en los delitos mencionados"[22].

- Artículo 9: *"(…) busca penalizar las conductas de Grooming, esto es, una nueva "forma de acoso y abuso hacia niños, jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente,*

[22] Idem.

por una de la misma edad de niño con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual" . Casos en los cuales, los menores quedan desprotegidos, vulnerables, y en algunos casos, sujetos a la sextorsión subsiguiente, en la cual la persona que tienen en su poder las fotos, constriñe al menor de entregar más so pena de revelar las ya entregadas. Con este propósito, se busca proteger a los menores de edad de las amenazas emergentes en el mundo digital mediante la creación de este delito nuevo. Este artículo se centra en el acoso virtual, una forma de explotación que ha crecido con el auge de las tecnologías de la información y la comunicación.

El delito de acoso virtual se caracteriza por el contacto con un menor de edad a través de internet, redes sociales, o cualquier otro medio o red de información, comunicación o sistema informático. El objetivo del acosador es obtener imágenes, grabaciones audiovisuales o cualquier representación de contenido sexual del menor. Además, el acosador puede realizar 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.

El artículo establece una pena de prisión de setenta y dos (72) a ciento veinte (120) meses para aquellos que cometan este delito. Esta pena se aplica sin perjuicio de las demás sanciones penales a que hubiere lugar por el desarrollo de su conducta. Además, el artículo también penaliza a aquellos que, utilizando los mismos medios, contacten con un menor de edad y, mediante coacción, intimidación o engaño, busquen obtener cualquier tipo de provecho sexual. Esta disposición se aplica sin perjuicio de las correspondientes por la comisión de otros delitos derivados de estas conductas"[23].

- Artículo 10: *"(…) adiciona circunstancias de agravación específicas en casos de constreñimiento que involucren la amenaza de publicar contenido sexual de la víctima, con un enfoque particular en la protección de menores de dieciocho años, ampliando las herramientas legales para combatir la extorsión y otros delitos relacionados"*[24].

- Artículo 11: *"(…) consagra la creación de una medida cautelar que permita a la fiscalía solicitar a un juez de control de garantías el bloqueo preventivo de una URL*

[23] Idem.
[24] Idem.

cuando estime que por medio de esta se está cometiendo una conducta punible. En materia de procedimiento penal el Alto Tribunal ha establecido que, en virtud de la cláusula de competencia general, él tiene facultades para determinar los asuntos propios de los procedimientos judiciales, incluidos los deberes y las cargas procesales.

En esta labor el legislador deberá tener en cuenta los derechos y los principios constitucionales como límites a su facultad de reglamentación. Así pues, al momento de regular procedimientos es necesario tener en cuenta que las normas (i) no vulneren los límites propios de los principios y los fines del Estado, (ii) velen por la vigencia de los derechos fundamentales, (iii) permitan o materialicen derechos y el principio de primacía de lo sustancial sobre las formas, y (iv) que las disposiciones sigan el principio de razonabilidad.
En atención a esas reglas jurisprudenciales, la medida cautelar de bloqueo de los dominios de internet, URL, cuentas y usuarios, no vulnera los límites propios de los principios y fines del Estado. Por el contrario, pretende materializarlos al evitar la continuidad de afectaciones a bienes jurídicos de los niños, niñas y adolescentes sin necesidad de haber determinado la responsabilidad de las personas investigadas por la conducta, pero con evidencia suficiente sobre la materialidad de la conducta investigada.

El bloqueo de estos instrumentos cuando son utilizados para delinquir, propende por la vigencia del derecho fundamental de acceso a la justicia de las personas que han sido afectadas con esas conductas, y otorga especial importancia a lo sustancial que es evitar la comisión de nuevos delitos por esa vía. Adicionalmente, es importante señalar que resulta razonable imponer límites al uso de la tecnología, cuando se comprueba que ha sido instrumentalizada para afectar derechos de terceros.

De igual forma la posibilidad de crear mecanismos de investigación a través de la tecnología implica dotar de facultades suficientes y razonables al Ente Acusador para que materialice la justicia como un fin constitucional. A través de estas nuevas medidas de carácter normativo será posible materializar el derecho a la verdad de las víctimas, desarticular de manera efectiva las organizaciones criminales, y de esta forma contribuir a garantizar la convivencia pacífica.

La razonabilidad de la medida está trazada por el acceso masivo de las personas a los distintos avances de la tecnología, lo que les permite evadir los controles de las autoridades, y borrar los registros de sus conductas. Este escenario hace indefectible

otorgar a las autoridades suficientes facultades para investigar y judicializar la comisión de esas conductas. En conclusión, las medidas tanto penales como procedimentales que pretenden reducir la cibercriminalidad están plenamente ajustadas a la Constitución.

Además, es necesario señalar que, el Consejo Superior de Política Criminal ha dicho referente a la medida que: "resulta necesaria la implementación de medidas procedimentales que permitan a las autoridades competentes combatir este fenómeno de manera eficaz y eficiente, pues la legislación y los protocolos de policía judicial han quedado cortos ante este tipo de criminalidad""[25].

- Artículo 12: *"(…) actualiza el artículo 3° de la Ley 1146 de 2007, creando un Comité Interinstitucional Consultivo dedicado a la prevención de la violencia sexual y la atención integral de menores víctimas de abuso sexual, especificando su composición y objetivos para mejorar la coordinación y eficacia de las políticas públicas en esta materia"*[26].

- Artículo 13: *"(…) amplía las funciones de este Comité Interinstitucional Consultivo, asignándole la 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"*[27].

- 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"*[28].

IX. CONSTITUCIONALIDAD Y LEGALIDAD DEL PROYECTO

[25] Idem.
[26] Idem.
[27] Idem.
[28] Idem.

La exposición de motivos del Proyecto de Ley No. 254 de 2024 recalca que el legislador cuenta con un amplio margen de libertad en la configuración normativa de la política criminal y de los procedimientos aplicables, lo cual le permite adoptar medidas razonables para garantizar otros fines constitucionales. Afirma que las medidas penales y de procedimiento adoptadas en la iniciativa para hacer frente a la ciberdelincuencia cumplen con los requisitos constitucionales.

Con esto, procede a señalar el marco normativo que sustenta constitucional y legalmente la presente iniciativa, otorgando una minuciosa protección a los derechos de las niños, niñas y adolescentes:

- Constitución Política de 1991. Concretamente señala los siguientes artículos:

    - *"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"*[29].

    - *"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.*

      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"[30].

    - *"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,*

[29] Idem.
[30] Idem.

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.

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"[31].

- *"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"*[32].

- 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",* recalcando los siguientes artículos:

  - *"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"*[33].

  - *"Artículo 12. Medidas de sensibilización. Las autoridades de los distintos*

[31] Idem.
[32] Idem.
[33] Idem.

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.

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"[34].

- *"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"*[35].

- Ley 1098 de 2006 *"por la cual se expide el Código de la Infancia y la Adolescencia"*, concretamente el siguiente artículo:

  - *"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"*[36].

[34] Idem.
[35] Idem.
[36] Idem.

- 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"*, en particular el siguiente artículo:

    - *"Artículo 24. El artículo 218 de la Ley 599 quedará así:*

      Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor 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".

- 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"*, resaltando el siguiente artículo:

    - *"Artículo 2°. En el marco de la presente ley se entiende por:*

      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.

      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.

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.

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.

Ciberbullying 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"[37].

- Ley 1273 de 2009 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", en especial los siguientes artículos:

    - *"Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio 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"*[38].

[37] Idem.
[38] Idem.

- *"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"*[39].

- Ley 1928 de 2018 *"por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest."*.

X. IMPACTO FISCAL

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 ser óbice, para que las corporaciones públicas ejerzan su función legislativa y normativa.

Cabe resaltar que la iniciativa busca que las herramientas y autoridades existentes se articulen, unifiquen y mejores las estrategias de protección de los niños, niñas y adolescentes ante los delitos realizados a través de medios informáticos o electrónicos.

A pesar de no tener la información precisa sobre el gasto, se procede a hacer algunas aclaraciones sobre el impacto fiscal, en sometimiento al artículo 7° de la Ley 819 de 2003 y en concordancia con el Marco Fiscal de Mediano Plazo.

De acuerdo con el artículo 24 de la presente ley, los usos como las campañas y demás programas de prevención para delitos sexuales a cargo del Instituto Colombiano de Bienestar Familiar serán financiadas por el Fondo Contra la Explotación Sexual de

[39] Idem.

Menores (FCESM). Este Fondo estará asociado al gasto de inversión a cargo de la entidad en el Presupuesto General de la Nación de la siguiente vigencia, luego de que se apruebe el Proyecto de Ley.

En el mismo sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones deberá hacerse cargo de implementar el sistema de información contra delitos sexuales. Este nuevo sistema también estará a cargo del rubro de inversión de la entidad. Cabe aclarar que la ejecución del PGN 2023 del MinTIC presentó un indicador de Obligación sobre apropiación del 87%. Por esta razón, el anterior año faltó cerca de $14 mil millones de pesos; recursos suficientes para liderar el nuevo sistema de información.

XI. CONFLICTO DE INTERESES

Dando alcance a lo establecido en el artículo 3 de la Ley 2003 de 2019, "*Por la cual se modifica parcialmente la Ley 5 de 1992*", se hacen las siguientes consideraciones a fin de describir las circunstancias o eventos que podrían generar conflicto de interés en la discusión y votación de la presente iniciativa legislativa, de conformidad con el artículo 286 de la Ley 5 de 1992, modificado por el artículo 1 de la Ley 2003 de 2019, a cuyo tenor reza:

> "***Artículo 286. Régimen de conflicto de interés de los congresistas.*** *Todos los congresistas deberán declarar los conflictos de intereses que pudieran surgir en ejercicio de sus funciones.*
>
> *Se entiende como conflicto de interés una situación donde la discusión o votación de un proyecto de ley o acto legislativo o artículo, pueda resultar en un beneficio particular, actual y directo a favor del congresista.*
>
> *a) Beneficio particular: aquel que otorga un privilegio o genera ganancias o crea indemnizaciones económicas o elimina obligaciones a favor del congresista de las que no gozan el resto de los ciudadanos. Modifique normas que afecten investigaciones penales, disciplinarias, fiscales o administrativas a las que se encuentre formalmente vinculado.*

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

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

Sobre este asunto la Sala Plena Contenciosa Administrativa del Honorable Consejo de Estado en su sentencia 02830 del 16 de julio de 2019, M.P. Carlos Enrique Moreno Rubio, señaló que:

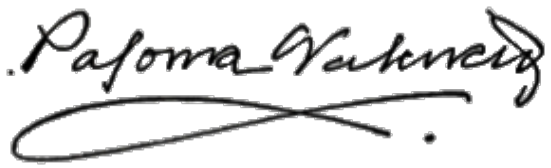
> *"No cualquier interés configura la causal de desinvestidura en comento, pues se sabe que sólo lo será aquél del que se pueda predicar que es directo, esto es, que per se el alegado beneficio, provecho o utilidad encuentre su fuente en el asunto que fue conocido por el legislador; particular, que el mismo sea específico o personal, bien para el congresista o quienes se encuentren relacionados con él; y actual o inmediato, que concurra para el momento en que ocurrió la participación o votación del congresista, lo que excluye sucesos contingentes, futuros o imprevisibles. También se tiene noticia que el interés puede ser de cualquier naturaleza, esto es, económico o moral, sin distinción alguna".*

Por lo anterior, se estima que este Proyecto de Ley no genera conflictos de interés para su discusión y votación, toda vez que se trata de un proyecto de carácter general que no crea un beneficio o perjuicio particular, actual y directo. No obstante lo anterior, es menester precisar que la descripción de los posibles conflictos de interés que se puedan presentar frente al trámite o votación del presente Proyecto de Ley, conforme a lo dispuesto en el artículo 291 de la Ley 5 de 1992 modificado por la Ley 2003 de 2019, no exime al Congresista de identificar causales adicionales en las que pueda estar inmerso.

XII. PROPOSICIÓN

En virtud de las anteriores consideraciones y en cumplimiento de los requisitos establecidos en la Ley 5ª de 1992, presento ponencia positiva y en consecuencia solicito a la los miembros de la Honorable Comisión Primera del Senado de la República **dar primer debate al 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"*, de conformidad con el texto original publicado en la Gaceta No. 233 de 2024.

Cordialmente,



PALOMA VALENCIA LASERNA
Senadora de la República
Ponente