MIRA
PARTIDO POLÍTICO

Copia

254/24

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 AGUDELO GARCÍA
Senadora de la República
Partido Político MIRA

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

MANUEL VIRGÜEZ PIRAQUIVE
Senador de la República
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:

1. 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.
2. 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.
3. Coordinación, concurrencia y subsidiariedad. Se refiere al tipo de relación y cooperación entre los diferentes niveles de la Administración Pública.
4. 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

1. 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 "sextorsión", edición de imágenes sexuales o "morphing",* ciberbullyng, 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 segun 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 prever, detectar identificar, y reducir las posibilidades de delitos informáticos contra niñas, niños y adolescentes que cuente con un Plan Anual de Seguridad.

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 cometan, 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 cometan 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

(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 constreñimiento 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

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 - colCERTo 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.

Parágrafo 2° El Comité promoverá la creación de Comités Regionales departamentales y/o municipales contra los delitos cibernéticos, los cuales estarán presididos por los correspondientes gobernadores o alcaldes, y que deberán contar también con una entidad que actuará como Secretaría Técnica. La Estrategia Nacional adoptada por el Comité será la base de su formulación de acción contra la Trata a nivel local haciendo los ajustes necesarios que consulten las especificidades del territorio y la población respectiva.

Artículo 13° Adiciónese varios numerales y un parágrafo nuevo al artículo 5° de la Ley 1146 de 2007 de la siguiente manera:

16. Adelantar y desarrollar las recomendaciones fundamentales para la política pública para la seguridad digital de los niños, niñas y adolescentes y realizar seguimiento a su ejecución.
17. Coordinar el proceso de revisión de los acuerdos y convenios internacionales relacionados con los delitos cibernéticos para supervisar su cumplimiento adecuado, y recomendar la firma de acuerdos, convenios o tratados necesarios para fortalecer la lucha contra la red.
18. Realizar estudios que permitan comprender las causas, consecuencias, formas de prevención y formas de protección a menores de edad en contra de los delitos cibernéticos y hacer las recomendaciones de normas o regulación del caso.

Artículo 14° ***Vigencia y derogatorias***. La presente ley rige a partir de su sanción y publicación, y deroga todas las normas que le sean contrarias.

Cordialmente,

ANA PAOLA AGUDELO GARCÍA
Senadora de la República
Partido Político MIRA

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

MANUEL VIRGÜEZ PIRAQUIVE
Senador de la República
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".

EXPOSICIÓN DE MOTIVOS

1. ANTECEDENTES.

Actualmente, se cuenta con 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". En el Concejo de Bogotá fue expedido como consecuencia 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 el año 2016 la iniciativa, Proyecto de Ley número 050 de 2016 Cámara, fue presentada ante el Congreso de la República por parte de la Bancada del Partido Político MIRA en esta Corporación y recibió conceptos y recomendaciones del Consejo Superior de Política Criminal, Ministerio de Educación Nacional, Instituto Colombiano de Bienestar Familiar.

Con estas recomendaciones, se presentó posteriormente 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", el cual se acumuló con el Proyecto de Ley 60 de 2018 Senado, 408 de 2019 Cámara denominado: "Proyecto de Seguridad Ciudadana".

De igual forma, encontramos como antecedentes otros proyectos como:

- Proyecto de ley No. 168/2020C de la Cámara: "Por medio de la cual se tipifica el delito de violencia sexual cibernética, y se dictan otras disposiciones". Autor: H.S Richard Aguilar

- Proyecto de ley No. 147/2023C de la 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". Autor: H.S.Nicolás Albeiro Echeverri Alvarán, H.R.Andrés Felipe Jiménez Vargas.

Actualmente, sobre la materia a regular, solo existen la 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; El artículo 56 de la Ley 1450 de 2011, que regula el principio de neutralidad en la Red. La Ley 1336 de 2009, que consagra disposiciones en la lucha y prevención de la pornografía infantil. Y, finalmente, la Ley 1273 de 2009, por medio de la cual se modificó el Código Penal, se creó un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos" el cual consagró varias modalidades ciber delictuales.

2. 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.

3. CONTEXTO

La masificación de las tecnologías de la información y de la comunicación ha permitido la participación mayoritaria de la ciudadanía en espacios virtuales en ejercicio de derechos de gran importancia como el acceso a la información pública, el habeas data y la intimidad. Esto significa que en la actualidad el Estado no solo tiene el deber de garantizar la convivencia pacífica de los ciudadanos en el territorio nacional, sino también en los espacios virtuales que estén bajo su control. Este 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.

La posibilidad de intercambiar información con otras personas sin una identificación real, las dificultades en materia de investigación y judicialización para determinar quién utilizó el mecanismo electrónico, la facilidad para alterar la evidencia, el carácter transnacional de las conductas, y la escasa conciencia de los usuarios sobre la necesidad de mantener unas mínimas medidas preventivas de seguridad, aunado a los bajos costos y riesgos que implican este tipo de operaciones, son algunos de los factores que han incentivado a los delincuentes a utilizar cada vez más las tecnologías de la información y de las comunicaciones para cometer conductas punibles.

Valga aclararse, que el presente proyecto de ley si bien regula delitos cometidos contra menores de edad. Además de proporcionar nuevas herramientas a la Fiscalía, con el fin de facilitar la efectiva investigación y judicialización de estos delitos.

4. IMPACTO ACTUAL DE CRÍMENES CIBERNÉTICOS EN EL MUNDO

El panorama global del bullying y ciberbullying, según el último estudio realizado por la ONG Internacional Bullying Sin Fronteras entre enero de 2022 y abril de 2023, revela una situación alarmante y creciente. Este estudio, con la colaboración de miles de estudiantes, profesores de prestigiosas universidades y la cooperación de hospitales y ministerios de educación, busca arrojar luz sobre la magnitud del problema en todo el mundo.

Los resultados del estudio son escalofriantes: el bullying y ciberbullying son descritos como "asesinos silenciosos" que cada año son responsables de la muerte de 200,000 niños y jóvenes en todo el mundo. Estos actos se alimentan de tres venenos: la soledad, la tristeza y el miedo, perpetuando un ciclo de sufrimiento entre las víctimas.

El informe destaca a México como el país con la mayor cantidad de casos registrados, con 270,000 incidentes graves de bullying y ciberbullying, representando un crecimiento del 50% respecto al informe anterior. Esto coloca a México en el primer lugar a nivel mundial, seguido por Estados Unidos y España, países que también presentan cifras alarmantes.

La ONG enfatiza que el bullying no se limita a los entornos físicos de las escuelas, sino que se ha extendido al ámbito digital, exacerbado por lo que se denomina las "4 Tóxicas": Twitter, Facebook, Instagram y WhatsApp, plataformas que permiten que el acoso continúe fuera del horario escolar, los fines de semana y durante las vacaciones, haciendo que las víctimas se sientan perseguidas sin

tregua.

Este estudio no solo busca informar sobre la gravedad y la prevalencia del bullying y ciberbullying en todo el mundo, sino también actuar como un llamado a la acción para combatir estos problemas. La visibilidad y el reconocimiento del bullying como un problema global urgente son pasos cruciales para desarrollar estrategias efectivas de prevención y apoyo a las víctimas.[1]

Según la UNICEF (2020), uno de cada cinco jóvenes dejaron de asistir al colegio debido a que sufrían un tipo de acoso en línea[2]. En América Latina siete de cada diez niños y adolescentes son víctimas de ciberacoso. El estudio además reveló que el 71% de los encuestados consideran que el acoso en Internet se da principalmente en las redes sociales.

A nivel mundial, Interpol realizó un examen en el 2018 encontrando las siguientes conclusiones: "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].Desde la Sociedad para la Prevención de la Crueldad de los Niños anuncian que con la llegada del Coronavirus han incrementado exponencialmente los casos de "online child abuse", igualmente, estiman 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].

En España, según un estudio de la Fundación ANAR y Fundación Mutua Madrileña, que recoge la opinión de 10.901 estudiantes y 491 docentes entre enero de 2020 y junio de 2021 concluyó que el ciberbullying es la forma de acoso que más presente ha estado desde que comenzó la pandemia, pues una cuarta parte de los alumnos afirma conocer compañeros de clase que podrían haberlo sufrido. Otra de las grandes conclusiones es que ahora 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%). Los motivos más frecuentes por los que se producen estas agresiones son el aspecto físico (52,5%), por ser diferente (46,4%), 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].

En el mismo país, en 2018 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] .

Según el estudio de Evaluación de la Amenza Global[7] en 2021 realizado por We Protect Global Alliance, revela que la explotación y el abuso sexual infantil se sigue proliferando. Muchas de las

---

[1](https://bullyingsinfronteras.blogspot.com/2023/09/estadisticas-mundiales-de-bullying.html

[2] 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]https://www.interpol.int/es/Delitos/Delitos-contra-menores/Base-de-datos-internacional-sobre-explotacion-sexual-de-menores

[4] https://www.theguardian.com/world/2020/apr/02/coronavirus-lockdown-raises-risk-of-online-child- abuse-charity-says

[5] https://www.rtve.es/noticias/20210915/acoso-escolar-agresiones-grupales-pandemia/2171018.shtml

[6] http://www.interior.gob.es/documents/10180/8736571/Informe+2018+sobre+la+Cibercriminalidad+en+Espa%C3%B1a.pdf/0cad792f-778e-4799-bb1f-206bd195bed2

[7] https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021-Report_Spanish.pdf

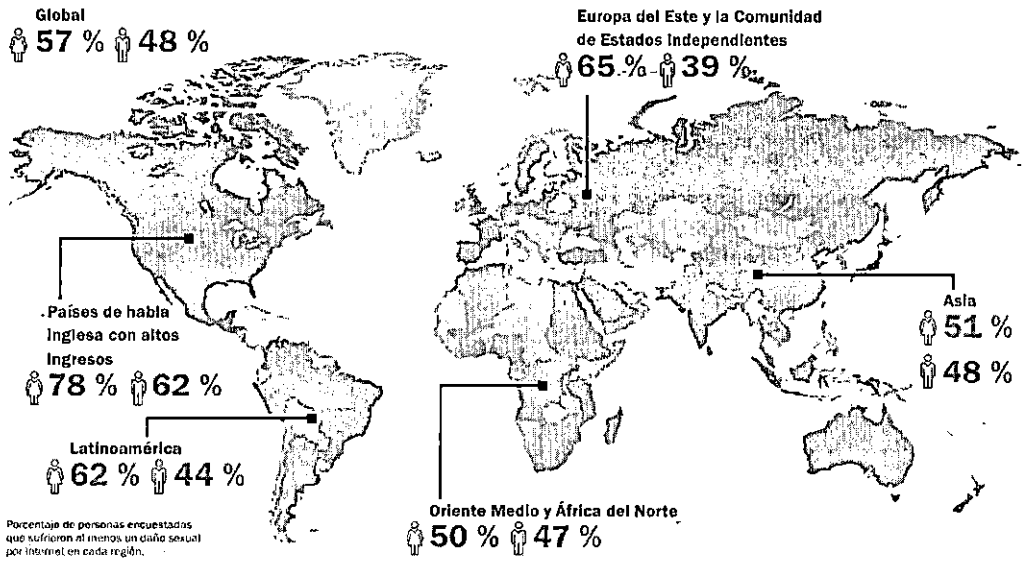
tendencias emergentes amenazan con incrementar aún más el volumen y la complejidad de los casos, agravando los retos de quienes trabajan para reducir el peligro y los daños. En cuando al ciberacoso, se detectó que enmayo de 2021, la Europol desmanteló una página web de abuso sexual infantil de la Dark 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).

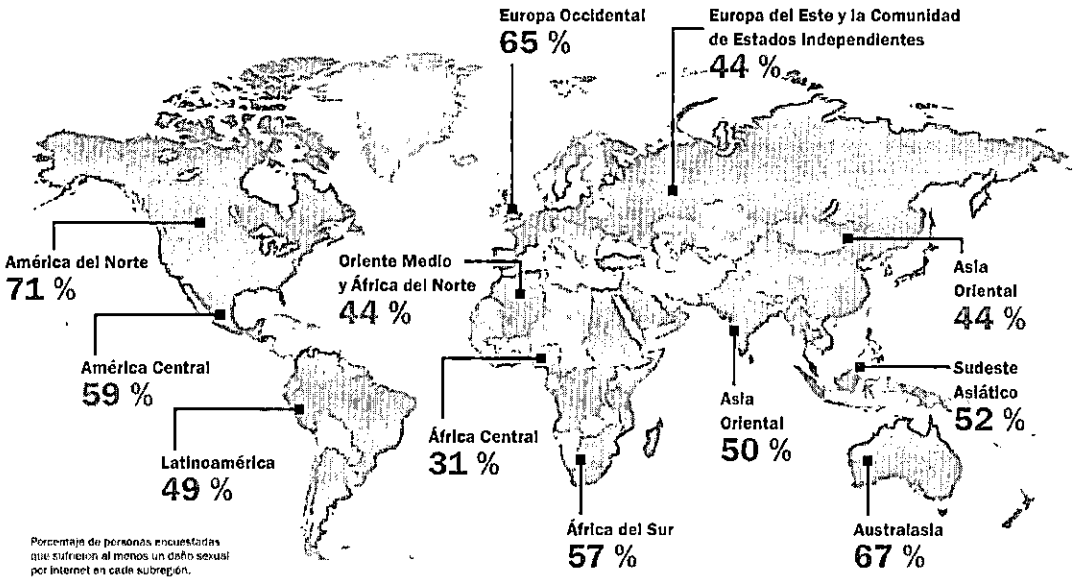
Gráfica 1.

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



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 cibercriminal, 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

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%20Annual%20Report%202022_SP.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 cómo 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 Policial[11], 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-vsKhSfA7zfYCwk-WFT2CBU/view?usp=sharing
[12] https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

productos en internet, que registraron 2,035 incidentes, mostrando una disminución significativa del 64%.

Además, el documento pone de relieve la falsedad personal en entornos digitales y las amenazas a través de redes sociales, con 875 y 806 incidentes respectivamente, marcando una disminución del 16% en ambos casos. 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.

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. 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. 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]

BOGOTÁ

Según la Cámara Colombiana de Informática y Telecomunicaciones, la capital colombiana registró un 28.4% de los delitos cibernéticos del país en 2022. En Bogotá 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

De acuerdo con 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 parte, todo el departamento de Cundinamarca ha denunciado 1.772 ciberdelitos, lo que equivale al 7.5% de los reportes.

Por lo anterior y en atención 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 en 2023 lanzó lo que denominó "Alerta en línea", una estrategia para prevenir "ciberdelitos" que afectan a jóvenes en Bogotá que involucra a estudiantes, docentes y 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].
La estrategia tuvo como objetivo reforzar la prevención de ciberdelitos como el "Grooming", el "Sexting" y el ciberacoso con la formación de estudiantes, docentes y padres de familia.

6. EXPLICACIÓN DEL ARTICULADO

El primer artículo 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

[13] https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023.pdf
[14] https://sci.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

criminales ejecutadas en el ciberespacio como delitos cibernéticos.

El segundo artículo 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.

El tercer artículo 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.

El cuarto artículo 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 competentes, para caracterizar las prácticas y delitos más comunes contra menores en el ámbito digital y fortalecer los mecanismos de denuncia e información.

El quinto artículo 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.

El sexto artículo 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.

El séptimo artículo 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.

El artículo octavo, 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;

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.

El artículo noveno, 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, 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"[15]. 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.

El 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.

[15] https://www.mintic.gov.co/portal/inicio/5626:Grooming

El artículo onceavo, 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 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".

El 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.

El 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.

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.

7. CONSTITUCIONALIDAD Y LEGALIDAD

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.

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:

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.

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.

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.

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.

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:

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.

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.

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.

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.

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.

Ley 1098 de 2006, por la cual se expide el Código de la Infancia y la Adolescencia
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.

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.
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.

Asimismo, el país cuenta con normatividad para proteger a las niñas, niños y adolescentes del ciberacoso o ciberbullying 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:

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.

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:
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".

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.

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.

Finalmente, se tiene la Ley 1928 de 2018 por medio de la cual Colombia se adhirió al convenio sobre la ciberdelincuencia "Convenio de Budapest".

8. 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 convertirse en 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.

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".

De los honorables congresistas,

ANA PAOLA AGUDELO GARCÍA
Senadora de la República
Partido Político MIRA

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

MANUEL VIRGÜEZ PIRAQUIVE
Senador de la República
Partido Político MIRA

CARLOS EDUARDO GUEVARA
Senador de la República
Partido Político MIRA

RADICACIÓN DEL PROYECTO DE LEY "POR MEDIO DE LA CUAL SE FORMULAN LINEAMIENTOS DE POLITICA PUBLICA PARA LA SEGURIDAD DIGITAL DE NIÑOS, NIÑAS, Y ADOLESCENTES, SE MODIFICA LA LEY 599 DE 2000 Y SE DICTAN OTRAS DISPOSICIONES"

CONGRESO DE LA REPÚBLICA

Secretaría General (Art. 139 y ss Ley 5ª de 1.992)

El día 12 del mes Marzo del año 2024 se radicó en este despacho el proyecto de ley N°. 254 Acto Legislatívo N°. _____, con todos y cada uno de los requisitos constitucionales y legales por: HS: Ana Paola Agudelo, Manuel Virgüez Carlos Eduardo Guevara HR: Irma luz Herrera

SECRETARIO GENERAL