Bogotá D.C., octubre de 2020

Doctor
**GREGORIO ELJACH PACHECO**
Secretario General
Senado de la República
Ciudad

**Asunto:** Radicación Proyecto de Ley.

Cordial saludo, respetado Doctor 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 Proyecto de Ley "*Por medio de la cual se expiden lineamientos en torno a la Seguridad Digital, se modifica 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,

**CARLOS EDUARDO GUEVARA V.**
Senador de la República
Partido Político MIRA

**AYDEÉ LIZARAZO CUBILLOS**
Senadora de la República
Partido Político MIRA

**MANUEL VIRGÜEZ P.**
Senador de la República
Partido Político MIRA

**IRMA LUZ HERRERA RODRIGUEZ**
Representante a la Cámara
Partido Político MIRA

CONGRESO DE LA REPÚBLICA DE COLOMBIA
SENADO DE LA REPÚBLICA

**PROYECTO DE LEY No. __ de 2020**

**"POR MEDIO DE LA CUAL SE EXPIDEN LINEAMIENTOS EN TORNO A LA SEGURIDAD DIGITAL, SE MODIFICA LA LEY 599 DE 2000, Y SE DICTAN OTRAS DISPOSICIONES".**

**Artículo 1. *Objeto*.** La presente Ley tiene por objeto 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, y determinar aquellas acciones dirigidas a prevenir estos delitos.

## CAPÍTULO I. DERECHOS Y DEBERES DIGITALES

**Artículo 2. *Deberes del Estado*.** Con respecto a la digitalidad, son deberes del Estado, entre otros:

1. Realizar capacitaciones y sensibilizar a todos los habitantes, con el fin de darles a conocer sus derechos y deberes digitales.
2. Generar políticas públicas de inclusión, a fin de lograr la mayor cobertura posible del servicio.
3. Diseñar planes de estudio para que desde los colegios se logre la inserción de los estudiantes en el mundo digital. Particularmente, estos planes de estudio deberán preparar a los estudiantes para afrontar los retos en esta materia y prevenir los riesgos digitales.

**Artículo 3. *Derechos digitales de los niños, niñas y adolescentes*.** Todos los niños, niñas y adolescentes tienen los siguientes derechos:

1. A que el sistema educativo garantice su efectivo aprendizaje de los medios digitales, de forma segura y respetuosa con los derechos fundamentales.
2. A acceder a actividades de prevención de los delitos cibernéticos, en los niveles de educación básica, media y superior.
3. A conocer la problemática de los delitos cibernéticos que se produce, tanto dentro del territorio nacional como fuera de él, a través de medios de difusión masiva.
4. A que sus profesores tengan las competencias digitales y la formación requerida para la enseñanza y transmisión de los valores y derechos.
5. A una navegación segura en Internet que permita su libre desarrollo a la personalidad.
6. A no ser constreñidos o incitados por terceros a realizar prácticas sexuales por Internet.
7. A que sus datos personales sean tratados con máxima diligencia.
8. Los demás que les asigne la ley.

**Parágrafo 1.** El Ministerio de Educación expedirá la reglamentación para el cumplimiento de los derechos mencionados en el artículo 1, 2 y 3, dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.

**Parágrafo 2.** El Ministerio del Trabajo reglamentará la forma en que se capacitará a los profesores conforme a lo reseñado en el numeral 4 dentro de los seis (06) meses posteriores a la entrada en vigencia de la presente ley.

## CAPÍTULO II. DISPOSICIONES PENALES

**Artículo 4.** 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 5.** Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

**Artículo 210C. *Grooming*.** El que haciéndose pasar por otra persona, o habiendo mentido sobre sus datos personales obtenga imágenes o grabaciones audiovisuales de la actividad sexual o con contenido sexual de un menor de edad, incurrirá en prisión de setenta y dos (72), a ciento veinte (120) meses, sin perjuicio de la pena que le corresponda por los demás delitos que se ocasionen con esta conducta.

**Artículo 6.** Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

**Artículo 228A. *Ciber-acoso*.** El que, sistemáticamente, usando cualquier medio o red de información o de comunicación, con el fin de causar daño o intimidación a otro promueva o difunda noticias falsas, imágenes o grabaciones audiovisuales, con contenido sensible sin consentimiento de su titular, o que incentiven al odio, incurrirá en multa.

**Artículo 7.** Adiciónese un nuevo numeral al artículo 240 de la Ley 599 de 2000, el cual quedará así:

**Artículo 240. *Hurto Calificado*.**
(...)
**5.** Prevaliéndose de datos personales a los que tuviere acceso en razón o con ocasión de su empleo, oficio o profesión.

**Artículo 8**. Modifíquese el numeral 4 del artículo 241 de la Ley 599 de 2000, el cual quedará así:

**Artículo 241.** ***Circunstancias de agravación punitiva.***
(...)
4. Por persona disfrazada, o aduciendo calidad supuesta, o simulando autoridad o invocando falsa orden de la misma**, o aprovechándose de uniforme o de signo distintivo de personas jurídicas, ONG's, empresas, o plataformas virtuales**.

**Artículo 9.** 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 10.** Adiciónese un nuevo numeral al artículo 247 de la Ley 599 de 2000, el cual quedará así:

**Artículo 247.** ***Circunstancias de agravación punitiva.***
(...)
**7.** La conducta se realice a través de medios informáticos, electrónicos o telemáticos, o cualquier técnica de manipulación informática.

**Artículo 11.** Modifíquese el artículo 269E de la Ley 599 de 2000, el cual quedará así:

**Artículo 269E.** ***Uso de software malicioso.*** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, **use**, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos 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 12.** Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

**Artículo 296A.** ***Falsedad personal usando medios tecnológicos.*** El que, sin consentimiento del sujeto pasivo, y valiéndose de medios tecnológicos, creare imágenes o videos en los que se simula el rostro de otra persona, y posteriormente los difundiere o publicare o a través de cualquier medio o red de información o de comunicación, con el propósito de obtener algún provecho económico, social o político, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses.

**Artículo 13.** Adiciónese un artículo nuevo a la Ley 599 de 2000, el cual quedará así:

**Artículo 374B. *Disposiciones comunes.*** Cuando las conductas de los artículos 372, 373 y 374 se cometan a través de cualquier medio, red de información o de comunicación o plataforma digital destinada para tal fin, la pena se aumentará en una tercera parte.

**Artículo 14.** 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.

**Artículo 15.** Modifíquese el artículo 38 de la ley 1801 de 2016, el cual quedará así:

**Artículo 38. *Comportamientos que afectan la integridad de niños, niñas y adolescentes.*** Los siguientes comportamientos afectan la integridad de los niños, niñas y adolescentes y por lo tanto no deben realizarse. Su incumplimiento da lugar a medidas correctivas, sin perjuicio de lo establecido por la normatividad vigente sobre la materia y de la responsabilidad penal a que haya lugar:

1. Permitir, auspiciar, tolerar, inducir o constreñir el ingreso de los niños, niñas y adolescentes a los lugares donde:
a) Se realicen espectáculos o actividades cinematográficas aptas solo para mayores de 18 años;
b) Se preste el servicio de videojuegos, salvo que sean aptos para la edad del niño, niña o adolescente, en las condiciones establecidas por la Ley 1554 de 2012;
c) Se practiquen actividades peligrosas, de acuerdo con la reglamentación establecida por el Gobierno Nacional;
d) Se realicen actividades sexuales o pornográficas, o se ejerza la prostitución, o la explotación sexual;

e) Se realicen actividades de diversión destinadas al consumo de bebidas alcohólicas y consumo de cigarrillo, tabaco y sus derivados y sustancias psicoactivas;
f) Se desarrollen juegos de suerte y azar localizados;

2. Inducir, engañar o realizar cualquier acción para que los niños, niñas y adolescentes ingresen o participen de actividades que les están prohibidas por las normas vigentes.

3. Permitir o inducir a los niños, niñas y adolescentes a utilizar las telecomunicaciones, publicaciones y documentos para acceder a material pornográfico.

4. Emplear o inducir a los niños, niñas y adolescentes a utilizar indebidamente las telecomunicaciones o sistemas de emergencia.

5. Facilitar, distribuir, ofrecer, comercializar, prestar o alquilar, cualquiera de los siguientes elementos, sustancias o bebidas, a niños, niñas o adolescentes:
a) Material pornográfico;
b) Bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;
c) Pólvora o sustancias prohibidas;
d) Armas, neumáticas o de aire, o que se asimilen a estas, elementos cortantes, punzantes, contundentes o sus combinaciones;

6. Inducir a niños, niñas o adolescentes a:
a) Consumir bebidas alcohólicas, cigarrillo, tabaco y sus derivados, sustancias psicoactivas o cualquier sustancia que afecte su salud;
b) Participar en juegos de suerte y azar;
c) Ingresar a fiestas o eventos similares en los cuales exista previa restricción de edad por parte de las autoridades de policía, o esté prohibido su ingreso por las normas vigentes.
d) La explotación laboral.

7. Permitir que los niños, niñas y adolescentes sean tenedores de animales potencialmente peligrosos.

8. Ejercer, permitir, favorecer o propiciar el abuso, los actos y la explotación sexual de niños, niñas o adolescentes.

9. Utilizar a niños, niñas y adolescentes para evitar el cumplimiento de una orden de policía.

10. Permitir que los niños, niñas y adolescentes hagan uso de piscinas y estructuras similares, de uso colectivo o de propiedad privada unihabitacional, sin el cumplimiento de los requisitos establecidos por la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.
11. Permitir que los niños, niñas y adolescentes sean parte de confrontaciones violentas que puedan derivar en agresiones físicas.

**12. Acceder a un sistema informático para impedir u obstaculizar el normal funcionamiento de las clases.**

**Parágrafo 1o**. En los comportamientos señalados en el literal b) del numeral 1 del presente artículo, se impondrá solo la medida correctiva de suspensión temporal de actividad y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1554 de 2012 y las normas que la adicionen o modifiquen.

**Parágrafo 2o**. En los comportamientos señalados en el literal d) del numeral 1 del presente artículo, será procedente también la medida correctiva de suspensión definitiva de la actividad.

**Parágrafo 3o.** En los comportamientos señalados en el literal d) del numeral 1 y en el numeral 8, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en las Leyes 679 de 2001, 1236 de 2008, 1329 de 2009 y las normas que las adicionen o modifiquen.

**Parágrafo 4o.** En los comportamientos señalados en el numeral 10, se impondrán las medidas correctivas en el presente Código y se pondrá en conocimiento de manera inmediata a la autoridad competente para aplicar lo establecido en la Ley 1209 de 2008 y las normas que la adicionen o modifiquen.

**Parágrafo 5o.** En los casos en los que los derechos de los niños, niñas y adolescentes se encuentren amenazados, inobservados o vulnerados se aplicará lo dispuesto en la Ley 109 2006.

**Parágrafo 6o.** A quien incurra en uno o más de los comportamientos antes señalados, se le aplicarán las siguientes medidas correctivas:

| COMPORTAMIENTOS | MEDIDA CORRECTIVA A APLICAR |
|---|---|
| Numeral 1 | Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien. |
| Numeral 2 | Multa General tipo 4; Suspensión temporal de actividad. |
| Numeral 3 | Multa General tipo 4; Destrucción de bien. |
| Numeral 4 | Multa General tipo 1. |
| Numeral 5 | Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien. |
| Numeral 6 | Multa General tipo 4; Suspensión temporal de actividad; Destrucción de bien. |
| Numeral 7 | Multa General tipo 2. |
| Numeral 8 | Suspensión definitiva de actividad. |

| | |
|---|---|
| Numeral 9 | Multa General tipo 4. |
| Numeral 10 | Suspensión temporal de actividad. |
| Numeral 11 | Multa General tipo 4. |
| **Numeral 12** | **Multa General tipo 4; Participación en programa comunitario o actividad pedagógica de convivencia.** |

**Parágrafo 7o.** Al menor de 18 años que cometa cualquiera de los anteriores comportamientos se le aplicarán las medidas previstas en el Código de infancia y adolescencia.

**Parágrafo 8o.** Quien en el término de un año contado a partir de la aplicación de la medida, reincida en alguno de los comportamientos prohibidos en el presente capítulo que dan lugar a la medida de suspensión temporal, será objeto de suspensión definitiva de la actividad.

**Parágrafo 9o. En el comportamiento de sabotaje descrito en el numeral 12, se realizará la compulsa de copias a la Fiscalía General de la Nación, cuando como forma de sabotaje se reproduzca material pornográfico.**

## CAPÍTULO III. DISPOSICIONES FINALES.

**Artículo 16.** ***Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos***. Créese el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos. Su integración y funciones se regirán por lo dispuesto en la presente ley. El Comité será el organismo consultivo del Gobierno Nacional y el ente coordinador de las acciones que desarrolle el estado colombiano, a través de la estrategia nacional para la lucha contra los delitos cibernéticos.

**Artículo 17.** ***Integración del Comité.*** El Comité estará integrado por los siguientes miembros:

1. La Fiscalía General de la Nación o quien hiciera sus veces, quien lo presidirá.
2. El Ministerio de Relaciones Exteriores o el Director de Asuntos Consulares y de Comunidades Colombianas en el Exterior, o quien hiciera sus veces.
3. El Ministerio de Educación o quien hiciera sus veces.
4. La Comisión Reguladora de Comunicaciones o quien hiciera sus veces
5. La Policía Nacional o quien hiciera sus veces
6. El Ministerio de las Tecnologías de la Información y de las Comunicaciones o quien hiciera sus veces.
7. El Ministerio de Justicia y del Derecho o quien hiciera sus veces.
8. La Procuraduría General de la Nación o quien hiciera sus veces.
9. La Defensoría del Pueblo o quien hiciera sus veces.
10. El Subdirector General de la Oficina de Interpol en Colombia o quien hiciera sus veces.
11. El Instituto Colombiano de Bienestar Familiar o quien hiciera sus veces.

12. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT o quien hiciera sus veces.
13. Consejería Presidencial para la Niñez y Adolescencia o quien hiciera sus veces.
14. Consejería Presidencial para los Derechos Humanos y Asuntos Internacionales quien hiciera sus veces.
15. Consejería presidencial para asuntos económicos y transformación digital.

**Parágrafo 1**. 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.

**Parágrafo 2.** El Comité podrá invitar a sus sesiones a cualquier otra entidad del Estado, personas jurídicas de derecho privado y organizaciones internacionales, que tengan por objeto la lucha contra los delitos cibernéticos, o la protección de los Derechos Humanos de las víctimas del mismo, organizaciones que tengan por objeto la promoción y defensa de los derechos humanos, y a particulares cuya presencia sea conveniente para el cumplimiento de las funciones propias del Comité.

**Parágrafo 3**. Los integrantes mencionados deberán mencionar las actividades que realizaren siendo parte del Comité, en su respectiva rendición de cuentas, cuando hubiere lugar a ello.

**Artículo 18. *Funciones*.** El Comité Interinstitucional para la lucha contra los delitos cibernéticos ejercerá las siguientes funciones:

1. Desarrollar la estrategia nacional contra los delitos cibernéticos y realizar seguimiento a su ejecución

2. 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.

3. Actuar como órgano asesor y recomendar acciones a las entidades que se dedican directa o indirectamente a la lucha contra el delito cibernético.

4. Actuar como organismo coordinador de entidades nacionales y organizaciones privadas involucradas en la implementación de la Estrategia Nacional, frente a las acciones interinstitucionales que deben tomarse.

5. Formular recomendaciones en materia de persecución criminal de los delitos cibernéticos y del fortalecimiento de la capacidad del Estado en este campo.

6. Recomendar la expedición de normas o regulaciones a las distintas entidades del Estado en materia de delitos cibernéticos.

7. 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.

8. Realizar las respectivas compulsas de copias de conductas delictivas a las que tuvieren conocimiento.

9. Diseñar estrategias internacionales que permitan la adecuada persecución criminal de los delitos cibernéticos.

10. Diseñar su propio plan de acción y dictar su reglamento interno.

**Parágrafo**. Podrán crearse grupos especializados en las distintas áreas de los delitos cibernéticos.

**Artículo 19.** ***Funcionamiento del Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos.*** Para el desarrollo de las funciones del Comité se creará la secretaría técnica a cargo del ministerio de justicia, quien podrá delegarla en la dependencia que para el efecto éste designe, sin que ello implique el incremento de funcionarios en su planta de personal. Esta secretaría es de carácter permanente. El Comité se reunirá en forma ordinaria por lo menos una vez cada dos meses, por convocatoria de la Secretaría Técnica. El Comité también se podrá reunir extraordinariamente cuando el presidente del Comité lo considere pertinente. La secretaría técnica rendirá informes bimestrales a los integrantes del Comité sobre su funcionamiento y las acciones adelantadas para dar cumplimiento a la presente ley. También rendirá informes anuales al Presidente de la República en el mismo sentido.

**Artículo 20.** ***Estrategia Nacional contra los Delitos Cibernéticos.*** El Gobierno Nacional adoptará mediante la Estrategia Nacional contra los Delitos Cibernéticos. El Comité Interinstitucional de que trata el artículo 16 de la presente ley, conformado para la Lucha contra los delitos cibernéticos formulará la estrategia nacional. Las ramas del poder público u órganos autónomos que deban intervenir en la implementación de las acciones de la presente estrategia, lo harán por medio del director correspondiente mediante acto administrativo. Los objetivos de la presente estrategia serán:

1. Desarrollar marcos de información relativa a las causas, modalidades, particularidades regionales y consecuencias de los delitos cibernéticos.

2. Prevenir los delitos cibernéticos a través de medidas sociales y pedagógicas.

3. Fortalecer las acciones de persecución a organizaciones criminales y, en general, la investigación, judicialización y sanción de los delitos cibernéticos.

4. Proteger y asistir a las víctimas de los delitos cibernéticos, en los campos físico, psicológico, social, económico y jurídico.

5. Promover el trabajo interinstitucional y la cooperación internacional en la lucha contra los delitos cibernéticos.

6. Los demás que el Comité Interinstitucional considere necesarios.

**Parágrafo.** La Estrategia Nacional medirá periódicamente el cumplimiento de los objetivos, así como el impacto, la eficacia y la eficiencia de la implementación de la estrategia mediante metas e indicadores de gestión.

**Artículo 21**. ***Mecanismos de prevención de los delitos cibernéticos.*** La Estrategia Nacional contra los Delitos Cibernéticos establecerá la ejecución masiva de campañas y programas de prevención de los delitos cibernéticos, las cuales incluirán los factores más comunes, los medios de protección y la forma de denunciarlos. Estos mecanismos estarán a cargo del Gobierno Nacional, sus instituciones judiciales y de policía, y las autoridades nacionales y territoriales.

**Artículo 22. *Articulación en la investigación judicial y la acción policiva*.** El Ministerio de Defensa en coordinación con la Fiscalía General de la Nación realizarán capacitaciones especializadas para la investigación y persecución de los delitos cibernéticos, promoviendo la cooperación internacional en los ámbitos judiciales y policivos, respecto a los delitos cibernéticos. Estas entidades elaborarán informes anuales para el Comité Interinstitucional para la Lucha contra los Delitos Cibernéticos, con el objetivo de contribuir a una orientación de las decisiones.

**Artículo 23. *Vigencia y derogatorias***. La presente ley rige a partir de su sanción y publicación, y deroga todas las normas que le sean contrarias.

De los honorables Congresistas,

**CARLOS EDUARDO GUEVARA V.**
Senador de la República
Partido Político MIRA

**AYDEÉ LIZARAZO CUBILLOS**
Senadora de la República
Partido Político MIRA

**MANUEL VIRGÜEZ P.**
Senador de la República
Partido Político MIRA

**IRMA LUZ HERRERA RODRÍGUEZ**
Representante a la Cámara
Partido Político MIRA

**PROYECTO DE LEY No. __ de 2020**

**"POR MEDIO DE LA CUAL SE EXPIDEN LINEAMIENTOS EN TORNO A LA SEGURIDAD DIGITAL, SE MODIFICA 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".

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 clasificar y tipificar cómo delitos cibernéticos nuevas acciones criminales ejecutadas en el ciberespacio, así como acciones estatales para prevenirlos.

## 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, no se circunscribe estrictamente a ellos. Busca regular de manera integral nuevas modalidades delictuales no contenidas en la regulación de hoy. 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

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"[1].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[2].

La Policía de Inglaterra ha señalado que, comparado a 2018, el periodo 2019-2020 ha tenido un aumento en las conductas de "online child abuse" esto es, ciber delitos[3]. Igualmente, el FBI en E.E.U.U. ha encontrado un incremento alarmante en la comisión de estos delitos en un 60% con una agravante, cada sujeto capturado realiza sus actos criminales con hasta 300 niños[4].

En España, 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

[1] https://www.interpol.int/es/Delitos/Delitos-contra-menores/Base-de-datos-internacional-sobre-explotacion-sexual-de-menores
[2] https://www.theguardian.com/world/2020/apr/02/coronavirus-lockdown-raises-risk-of-online-child-abuse-charity-says
[3]https://www.scotland.police.uk/whats-happening/news/2020/april/child-sexual-abuse-campaign
[4] https://www.fbi.gov/audio-repository/ftw-podcast-sextortion-activity-on-rise-053019.mp3/view

conjunto de la criminalidad. Como se puede observar en la tabla nº 1, hemos pasado del año 2011, donde nos situábamos en el 2,1% al año 2018 con el 7,0%"[5] .

| | |
|---|---|
| 2011 | 2,1% |
| 2012 | 2,5% |
| 2013 | 2,6% |
| 2014 | 3,1% |
| 2015 | 3,9% |
| 2016 | 4,3% |
| 2017 | 5,3% |
| 2018 | 7,0% |

Adicionalmente, se tiene que para el año 2018 "las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de 84.60715, es decir, un 35,5% más que en el año 2017", y hoy "Las Fuerzas de Seguridad detectaron 218.302 ciberdelitos en 2019"[6]. Notándose así un aumento considerable de los ciberdelitos. Por su parte, en Estados Unidos, el Centro de Quejas por Delitos en Internet (IC3) recibió 467,361 quejas en 2019, un promedio de casi 1,300 por día, y registró más de $ 3.5 mil millones en pérdidas para víctimas individuales y comerciales.[7]

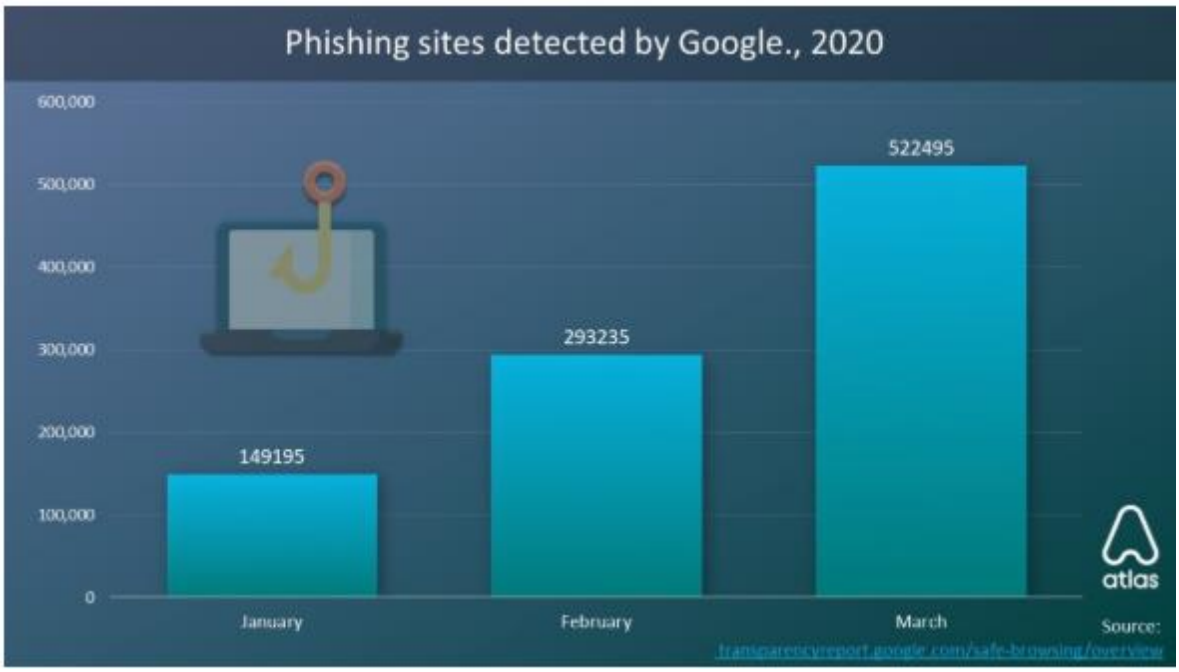
Organizaciones internacionales, señalan la urgencia de tomar medidas en contra de los ciber delitos, en concreto la UNCIRTRI (por sus siglas en inglés) señala que "Las técnicas comunes de cibercrimen, como el phishing, han experimentado un aumento. (…) Según el informe, en enero, Google registró 149k sitios web activos de phishing. En febrero, ese número casi se duplicó a 293k. Sin embargo, en marzo, ese número aumentó a 522k, un aumento del 350% desde enero."[8] (traducción propia), Informe que se representa en la siguiente tabla:

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

[6] http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/11966023

[7] https://pdf.ic3.gov/2019_IC3Report.pdf

[8] http://www.unicri.it/news/article/covid19_cyber_crime




Señala la UNCITRI que "**Países de todo el mundo informan un aumento en el cibercrimen durante la pandemia**. Por ejemplo, en Italia, la Polizia Postale, que es la rama de aplicación de la ley a cargo de los delitos cibernéticos, informó varios tipos de estafas y fraudes que llegaron en forma de anuncios, correos electrónicos, sitios web falsos, pero también a través de llamadas telefónicas y mensajes Los ciberdelincuentes están aprovechando las ansiedades y los temores provocados por la pandemia, utilizando malware, como virus, gusanos, troyanos, ransomware y spyware, para invadir, dañar, robar o cancelar datos personales en computadoras personales. Los datos robados se pueden usar para diferentes propósitos maliciosos, incluido el acceso a cuentas bancarias y el chantaje a las víctimas a cambio de rescates. También se ha señalado un software "Corona antivirus" a las autoridades policiales italianas. La aplicación, BlackNet Rat, promete proteger el dispositivo del usuario del coronavirus, pero en cambio, viola la seguridad de la computadora y toma el control de la computadora, permitiendo que el delincuente lo controle de forma remota."[9].

La INTERPOL a su vez, advierte que "Los delincuentes prolíficos y oportunistas se están aprovechando de la pandemia de coronavirus COVID-19 para lanzar una variedad de Ataques cibernéticos"[10].

Frente a los crímenes de naturaleza sexual, vale aclararse que la EUROPOL ha encontrado nuevas formas de comisión de delitos contra menores, a saber:

"Redes punto a punto (P2P) y acceso anónimo como las redes Darknet (por ejemplo, Tor). Estos entornos informáticos siguen siendo la plataforma principal para acceder al material de abuso infantil y el medio principal para la distribución no comercial. Estos son invariablemente atractivos para los

[9] Íbid.
[10] https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

delincuentes y fáciles de usar. El mayor nivel de anonimato y las fuertes posibilidades de conexión en red que ofrece Internet oculto que existe debajo de la "red de superficie", parecen hacer que los delincuentes se sientan más cómodos al ofender y discutir sus intereses sexuales.

Transmisión en vivo de abuso sexual infantil. Facilitado por la nueva tecnología, una tendencia se refiere al abuso de niños con fines de lucro en el extranjero, en vivo frente a una cámara a pedido de los occidentales.

La transmisión de abuso en vivo a pedido"[11]. Al respecto, es válido preguntarse, qué acciones existen legalmente en Colombia que permita al ente investigador encontrar casos o diseñar alertas para cuando un menor esté siendo explotado sexualmente mediante links P2P.

Finalmente, 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"[12]

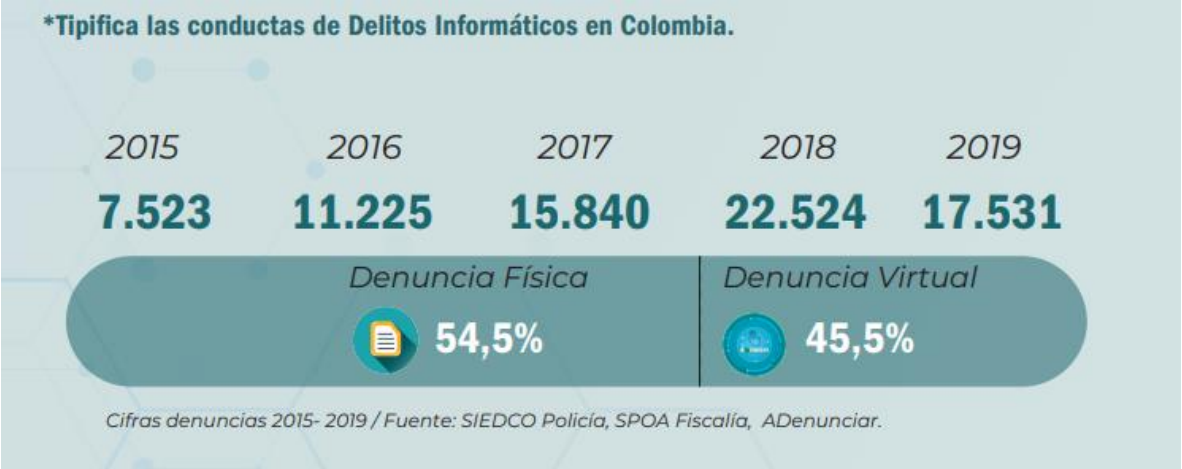
## 5. IMPACTO ACTUAL DE CRÍMENES CIBERNÉTICOS EN COLOMBIA

La Policía Nacional ha identificado un aumento sustancial de denuncias de la ciudadanía relacionada con amenazas de divulgación de información, relativa a la intimidad sexual de las personas, como mecanismo de presión para obtener beneficios económicos o de otra índole. Este tipo de conductas son reconocidas por la comunidad internacional como *sexting* y *sextorsión.*

De conformidad con los datos brindados por la Policía Nacional, entre 2016 y 2019, se reportaron en el CAI virtual 7.413 conductas de tipo sexual cometidas a través de la red en contra de niños, niñas y adolescentes. Tan solo en 2019 se cometieron 1.043 conductas, siendo las conductas no tipificadas las cometidas en mayor medida. Estas cifras son desoladoras, máxime cuando se trata solamente de las denuncias que han sido denunciadas, en la impunidad "cuántas conductas se cometerán" Lo que se evidencia hoy en día es que muchos delitos se cometen por medio de redes sociales como Twitter, Facebook, Instagram, donde hay muchas redes de pedófilos que aprovechan el anonimato y la facilidad de contacto para realizar estas conductas.

No obstante, no solamente preocupan las cifras de delitos sexuales cometidos a través de las redes. También la Cámara Colombiana de Informática y Telecomunicaciones ha encontrado un incremento del 54% entre 2018 y 2019 de la comisión de ciber delitos.[13] También presentan el siguiente gráfico.

[11] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
[12] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
[13] https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf




Con un aproximado de 60 denuncias diarias a nivel nacional, Bogotá encabeza el primer puesto como la ciudad con más ciber delitos denunciados, con un total de 5.308 casos en 2019. Se encuentra también un incremento del 612% en conductas de Malware. Por último, este informe de la CCIT encuentra como tendencias del delito los siguientes: Inteligencia Articial y Malware; Uso de perles falsos en redes sociales para difusión de Malware; BEC basado en Deepfake[14]; Uso de Botnet para difusión de correos extorsivos; Uso de mercados ilegales en DarkNet.

## 6. EXPLICACIÓN DEL ARTICULADO

El artículo primero es el objeto del proyecto. El segundo artículo consiste en darle al Estado una serie de obligaciones destinadas a garantizar progresivamente una cobertura integral de Internet a toda la población colombiana. En este sentido, es claro que, aunque el Gobierno Nacional ha tomado acciones positivas e iniciativas claras destinadas al mismo logro, hoy en día más de la mitad de la población colombiana[15] no cuenta con acceso a este servicio.

El artículo tercero estipula varios derechos digitales que tienen los niños, niñas y adolescentes, como consecuencia de la multiplicidad de tratados internacionales firmados por Colombia, además de la modernización y digitalización vividas actualmente que exigen el avance del Derecho, para no desproteger las garantías mínimas que deben revestir a estos seres de especial protección.

---

[14] Las empresas en Colombia podrán recibir audios e incluso videos, en los cuales los cibercriminales suplanten a ejecutivos, clientes y proveedores para conseguir transferencias de dinero o despacho de productos. La tecnología Deepfake es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces. Tomado de (https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf)

[15] De acuerdo con un informe realizado por el Centro Nacional de Consultoría (CNC), llamado 'Apropiación Digital 2020', cuatro de cada cinco colombianos (uno más que hace cuatro años) ya entraron en la era digital. Sin embargo, la mitad de la población limita el uso de la red a aspectos básicos como el entretenimiento y la comunicación. Tomado de (https://www.larepublica.co/internet-economy/aumenta-cobertura-de-internet-pero-mitad-de-la-poblacion-lo-usa-para-entretenerse-2977746)

El artículo cuarto, 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 a 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 quinto, 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"[16]. 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.

El artículo sexto, busca la creación del tipo penal de ciber acoso, también denominado, ciber bullying, como aquella forma de acoso que se produce de forma sistemática. Con esto no se está buscando restringir la libertad de expresión, no es posible tampoco usar este tipo penal como una forma de moción de opiniones, por ejemplo de columnas de opinión, o de manifestaciones hechas a través de

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

redes sociales. Puesto que, este tipo exige para su configuración la sistematicidad como requisito. Resulta claro, que, en todo caso, la libertad de expresión no cubre aquellos casos en los que, a manera de ejemplo, una persona envía correos electrónicos cada hora durante un año a un joven, con el fin de generar en él una idea suicida o simplemente causarle sufrimiento.

El artículo séptimo, busca regular situaciones que la pandemia ha generado, así, la cuarentena ha intensificado la necesidad de uso de plataformas digitales de domicilios, y en general, del uso de domicilios, consagra una calificante para aquellos casos en los que el delincuente tiene acceso a información personal de la víctima y en uso de ella comete el delito. Es decir, contempla aquellas conductas en las que los delincuentes se unen a las plataformas o redes de comunicación, de forma dolosa, con el único objetivo de conseguir información de potenciales víctimas. Así, se califica la conducta cuando en uso y violación de los datos personales se facilita la comisión del hurto.

El artículo octavo, igual que el anterior, busca regular situaciones que la pandemia ha intensificado, esto es, se ha aumentado el acercamiento de los delincuentes a dichas plataformas y redes de comunicación, quienes en uso y desprestigio de las mismas, cometen hurtos en las viviendas. Es decir, personas que portan un uniforme o un signo distintivo, con el fin de generar que su víctima baje la guardia, abra la puerta, o permita su ingreso al conjunto a fin de hurtarle. Cabe resaltar, que la disposición que se sugiere difiere del uso del disfraz, toda vez que el disfraz consiste en hacerse parecer algo que no se es. Situación totalmente distinta, a cuando efectivamente lo es. Es decir, una cosa es aparentar ser de cierta plataforma, y otra es efectivamente serlo. Situación última que se ha venido presentando en mayor medida y que no está consagrada al día de hoy por no tratarse de un disfraz.

El artículo noveno, consagra la modalidad delictual de la "sextorsión", en efecto, este delito se define como "la amenaza de enviar o publicar imágenes o videos con contenido sexual de una persona. Esto puede hacerse a través de teléfonos celulares o Internet"[17] Situación que al no estar regulada expresamente como delito, permite la rápida proliferación de este tipo de conductas, en otras palabras, al consagrar esta disposición como delito, se busca con ello lograr una prevención general en la población, con miras a disminuir la realización de estas conductas, pero además, con miras a efectuar una posible justicia restaurativa sobre los derechos de las víctimas. También, busca agravar aquellas extorsiones (sexuales o no) que se cometan contra menores de edad.

El artículo décimo, busca agravar los delitos de estafa cuando los mismos se produzcan de forma online, fundamentado en un mayor desvalor de acción objetivo, es decir, la facilidad que la tecnología y el anonimato le dan al delincuente de cometer el delito, y la dificultad para el Estado de perseguir y criminalizar estas conductas.

El artículo onceavo, busca incluir dentro del tipo penal de software malicioso el "uso", toda vez, que este verbo rector no se encontraba hoy regulado, siendo vital en la cadena de producción y comisión del delito.

El artículo doceavo, busca penalizar las conductas denominadas morphing (alteración de imágenes con fines sexuales) o también conocidas como Deep Faking (alteración de imágenes en general), en

[17] https://mintic.gov.co/portal/inicio/5786:Sextorsion

las que el sujeto activo prevaliéndose de herramientas como la inteligencia artificial o software altamente sofisticados logran la simulación exacta y real del rostro de otra persona con el fin de, por ejemplo, hacerlo decir cosas que no ha dicho. Este delito, a manera de ejemplo, puede ser usado para simular la voz o el rostro ante una entidad bancaria y lograr una transferencia no consentida de activos. O, por ejemplo, para hacer parecer que un Acalde o un Senador, o un Represente a la Cámara, ha dicho o hecho algo delictual y poder lograr una medida cautelar en su contra.

El artículo treceavo, consagra una disposición común a los delitos de los artículos 372, 37 y 374, con el fin de agravar las conductas allí cometidas, cuando las mismas se produzcan de forma online. Esto está fundamentado en un mayor desvalor de acción objetivo, por cuanto, facilita la conducta al delincuente, pues elimina las barreras de tener a la que buscar a la clientela, pues son los mismos clientes los que llegan a al vendedor por medios digitales. Y, además, dificulta la persecución criminal, pues la apariencia de legalidad de los negocios hace muy difícil su investigación. Cabe resaltar, que este delito no puede ser usado para perseguir al pequeño empresario o emprendedor, o al campesino que crea sus productos caseros, pues solo serán sujetos punibles quienes estén contenidos en los artículos 372, 373 y 374.

El artículo catorceavo, 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 quinceavo, busca regular una modalidad reciente que trajo consigo la pandemia. Aquellas situaciones en las que terceros ingresan a las clases virtuales con el fin de sabotearlas, o que mediante virus y demás artimañas logran infectar el equipo de los docentes, con el objetivo de impedir u obstaculizar dichas clases. Naturalmente, el auge exponencial de estas conductas obliga al Legislador a actuar y propender por medidas que permitan una adecuada convivencia, por este motivo se consagró dicha conducta como una contravención policiva.

Finalmente, el último capítulo contiene varios artículos cuyo objetivo es la creación de un Comité Interinstitucional, que permita un trabajo articulado entre todos los organismos estatales involucrados para una mejor respuesta y para la formulación de lineamientos y estrategias con miras a prevenir y reducir estos delitos.

No se niega la ardua labor del Estado colombiano a través del tiempo, como por ejemplo el CONPES 3071 de 2011, el CONPES 3854 de 2016, la Política Nacional de Ciberseguridad, los Centros de Respuesta a incidentes de Seguridad, y con la más reciente adhesión por parte del actual Gobierno al convenio de Budapest el cual es referente internacional contra la ciberdelincuencia. No obstante, las principales características de la ciberdelincuencia son, como lo recuerda Posada Maya[18], su capacidad de reinventarse y cambiar de forma diaria (lo que imposibilita el estudio de patrones para la efectiva investigación), la transnacionalidad propia de los delitos (un delincuente puede estar en este momento hurtando a 10 personas de distintos países al mismo tiempo), la inmediatez y la automaticidad de la conducta (un delincuente puede programar un computador para que cometa 10 delitos cada día, y el delincuente puede estar en otro lado en otra actividad, incluso a veces sin enterarse de sus propios delitos), el anonimato (propio de la era digital), la extrema sofisticación de los delincuentes en contravía de la poca preparación de los investigadores, entre muchas otras.

Todas estas características, exigen del Estado modelos de respuesta que en ningún caso pueden ser estáticos, y, que, además, deben ser integrales, los ciber delincuentes no lo son exclusivamente en el plano de seguridad estatal o en el plano de la ciber delincuencia económica. También, hay ciber

[18] POSADA MAYA, Ricardo. Los cibercrímenes: Un nuevo paradigma de criminalidad Un nuevo estudio del título VII bis del Código Penal Colombiano. Bogotá: Gustavo Ibáñez Carreño, 2017.

delincuentes que explotan sexualmente niños y niñas, también hay modalidades que puede que sean organizadas o no, pero que por su comisión permanente y elevada requieren respuestas eficaces con miras a disminuir, prevenir y en últimas criminalizar efectivamente.

## 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".

## 9. CIRCUNSTANCIAS O EVENTOS QUE PODRÍAN GENERAR CONFLICTOS DE INTERÉS.

De acuerdo con el artículo 3 de la Ley 2003 de 2019, atentamente nos disponemos a señalar algunos criterios guías en los que se podría configurar conflictos de intereses, para que los congresistas tomen una decisión en torno a si se encuentran inmersos en alguna de estas causales, sin embargo, pueden existir otras causales en las que se pueda encontrar cada congresista, las cuales deberán ser determinadas para cada caso en particular por su titular, siendo estos criterios meramente informativos y que deben ser analizados teniendo en cuenta lo expresado en el artículo 1 de la Ley 2003 de 2019.

Entre las situaciones que señala el artículo 1o antes mencionado, se encuentran: 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; y el 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*.".

Por lo anterior, las circunstancias o eventos que podrían generar un conflicto de interés, serían aquellos que tengan un beneficio particular, actual y directo, es decir, aquellos Congresistas que tengan investigaciones, procesos en curso o condenas por delitos contra la libertad, integridad y formación sexuales de los menores de edad.

De los honorables Congresistas,

**CARLOS EDUARDO GUEVARA V.**
Senador de la República
Partido Político MIRA

**AYDEÉ LIZARAZO CUBILLOS**
Senadora de la República
Partido Político MIRA

**MANUEL VIRGÜEZ P.**
Senador de la República
Partido Político MIRA

**IRMA LUZ HERRERA RODRÍGUEZ**
Representante a la Cámara
Partido Político MIRA