CONTRIBUCIÓN A LA RELATORÍA ESPECIAL DE NACIONES UNIDAS SOBRE LA VENTA Y EXPLOTACIÓN SEXUAL DE LOS NIÑOS

PRÁCTICAS EXISTENTES Y EMERGENTES DE EXPLOTACIÓN SEXUAL DE NIÑOS, NIÑAS Y ADOLESCENTES EN EL ENTORNO DIGITAL

PERSPECTIVA CHILENA Y GLOBAL

INTRODUCCIÓN

La colaboración del sector público y privado constituye un elemento esencial en la prevención, detección y protección frente a violencia en espacios digitales, cuyo norte ha de ser el respeto de los derechos humanos de niñas, niños y adolescentes (en adelante NNA) y la tecnología al servicio de las personas. Aunque se identifican claras responsabilidades de los Estados, como garantes de derechos, es indudable que el avance de las nuevas Tecnologías de la Información y de las Comunicaciones (en adelante TIC's) exigen no solo marcos regulatorios integrales, sino además medidas de diversa índole, así como alianzas público-privadas, que fomenten una responsabilidad social empresarial, una educación y/o alfabetización digital y que faciliten el uso responsable y seguro de tales entornos.

EXPLOTACIÓN SEXUAL DE NIÑOS, NIÑAS Y ADOLESCENTES EN EL ENTORNO DIGITAL

1. *Proporcione información sobre cómo se utilizan las tecnologías para facilitar la explotación y el abuso sexual de menores.*

En Chile, las principales actividades abusivas sexuales en el entorno digital contra niños, niñas y adolescentes se consuman mediante el uso de internet, específicamente mediante redes sociales y aplicaciones. En ello se identifica mayormente mensajes ofensivos, difusión de fotos, suplantación de identidad, preguntas del tipo sexual, hackeo y comentarios abusivos. En porcentajes, lideran: contenido sexual (61,5%), propuestas sexuales (57,8 %), comentarios con connotación sexual (59,5%), *grooming* (37,3%) y exposición sexual (28,0%). Si bien los delitos de producción de material abusivo no lideran las cifras, ha existido un aumento de denuncias ingresados a Ministerio Público, relevándose que la adquisición o almacenamiento lidera las cifras de casos policiales[i].

Por su parte, el uso de redes sociales y determinadas aplicaciones online facilitan la obtención de recursos monetarios por parte de NNA, entre ellas destacan "Tik Tok", "Instagram", "Only Fans" entre otras, que permiten subir imágenes de connotación erótico-sexual. Así mismo, la *DARK WEB* facilita que algoritmos de detección de violencia no sean detectados en redes sociales oficiales, depredadores camuflan ofrecimientos con mensajes sugerentes (no eróticos ni sexuales) pero que, al pincharlos, los reconducen a páginas de la *DARK WEB* exponiéndolos a visibilizar material abusivo. Otras formas de captación se realizan mediante agencias de modelaje, tales como las aplicaciones "Modelos Girls", "Sugar Daddy" y "Grindr", que permiten y normalizan el intercambio económico de imágenes y videos, contactos e interacciones que se concretan mediante mensajería privada[ii].

Finalmente, el uso de dispositivos móviles propios sin debida supervisión facilita exposición a conductas abusivas. El primer uso y entrega se realiza a muy temprana edad (antes de la edad recomendada, 10 años), este grupo prioriza internet para espacios de ocio y entretenimiento, superando tiempos máximos de conexión (más de 2 horas diarias recomendadas), falta de supervisión y alfabetización digital de adultos responsables y la mayoría de los NNA consumen contenido creado por terceros, sin información sobre los riesgos asociados en tales entornos[iii].

2. *¿Qué recomendaciones prácticas propondría a los Estados, la industria tecnológica y los proveedores de servicios en línea para prevenir la explotación y el abuso sexual de menores en el entorno digital?*

ESTADO

Diseñar y crear una política pública sobre desarrollo, uso seguro y responsable de las TiC's y entornos digitales que, comprenda ejes de promoción y prevención, con un claro enfoque en niñez, adolescencia y género, que impere y dialogue con Políticas y Planes Nacionales vigentes de Ciberseguridad e Inteligencia Artificial, como también considere ejes relativos a la promoción de investigación científica para el desarrollo de tecnologías de protección y su uso para mitigación de riesgos.

El plan de acción de dicha política debe considerar actividades de promoción, en especial, sobre alfabetización y educación digital segura y responsable, la difusión de campañas periódicas, tanto en plataformas digitales como en espacios educativos presenciales, para generar conciencia en el uso y riesgos asociados a estos entornos, debiendo ser, niños, niñas y adolescentes, co-garantes y usuarios, su público objetivo.

Se recomienda establecer estrategias de cooperación internacional que faciliten relaciones con instituciones especializadas en TIC's y ciberseguridad de países más avanzados, recogiendo experiencias positivas en la implementación de iniciativas y proyectos relacionados con ellas.

Crear un Consejo Público-Privado, como organismo técnico y especializado, para asesorar en el desarrollo, usos seguros y responsables de las TIC's y entornos digitales, que sirva de hoja ruta tanto para la creación e implementación de dicha política, promoviendo acuerdos, lineamientos estratégicos con el sector empresarial y con la participación de *stakeholders* relevantes, entre ellos, niños, niñas y adolescentes.[iv]

Promover regulaciones normativas respecto del acceso seguro de internet, ciberseguridad infantil, entornos digitales e inteligencia artificial, la que debe diseñarse sobre la base de evidencia técnica, que permita dar un marco regulatorio efectivo hacia la protección integral de niños, niñas y adolescentes. El marco normativo, debe considerar obligaciones preventivas y de protección para industrias de desarrollo tecnológico y proveedores de servicios y plataformas digitales, mandatándolos a adoptar medidas eficaces como: filtro y bloqueo de contenidos abusivos o sensibles, protección de datos, imágenes e información, protección de integridad, creación, difusión y promoción de controles parentales eficaces, estableciendo mecanismos efectivos de verificación de edad.

Crear una institucionalidad pública especializada, que cuente con facultades suficientes para que el Estado pueda ejercer su rol garante, en cuanto a control, fiscalización y sanción de dichas obligaciones.

INDUSTRIA TECNOLÓGICA Y PROVEEDORES

Incorporar en sus gobernanzas la sostenibilidad (ESG) promoviendo culturas organizacionales que fomenten conductas éticas y compromisos con el cumplimiento de buenas prácticas, estándares internacionales y la ley, bien sea en modelos de negocio relativos al desarrollo tecnológico y/o provisión de servicios de IA o digitales, considerando el impacto de dichas tecnologías, en los derechos de niños, niñas y adolescentes como *stakeholders* relevantes. Lo anterior exige fijar propósitos corporativos a largo plazo, creación de herramientas y líneas de defensa con debida diligencia, materialidad y participación significativa de estos grupos de interés y general alianzas pública-privadas.

Se recomienda además la creación de Códigos de Conducta para la protección de niños, niñas y adolescentes en internet, inversión en profesionales cualificados tanto en el diseño, implementación y gestión de productos o servicios, relevar modelos de *compliance* que incorporen en sus matrices de riesgos los relativos a impactos de dichos servicios o productos en niños, niñas y adolescentes, promover una cultura organizacional en ese sentido así como la colaboración con organismos especializados, ofrecer herramientas de controles parentales eficaces, monitoreo de medidas, y evaluación periódica para implementar mejoras. Reforzar los sistemas de vigilancia en la web, establecer políticas restrictivas sobre usos de dichas plataformas y difusión de canales de denuncia seguras y eficaces.

3. *¿Cuáles son las lagunas que siguen limitando la aplicación efectiva de las leyes, políticas y directrices existentes para prevenir, detectar, denunciar y proteger a los niños de la explotación y los abusos sexuales en línea?*

Desde la prevención: ausencia de legislación que regule entornos digitales, ciberseguridad infantil, inteligencia artificial, deberes y responsabilidad legal de personas jurídicas en ese sentido, así como la inexistencia de institucionalidad pública con facultades suficientes de control y fiscalización.

Así mismo, ausencia de política pública sobre desarrollo, uso seguro y responsable de entornos digitales y el déficit de enfoque en derechos de niñez y adolescencia en políticas y planes nacionales vigentes como los de Ciberseguridad y de Inteligencia Artificial. En el mismo sentido,

no existe política ni plan de promoción de una alfabetización y educación digital continua, se presentan brechas de especialización en violencia digital tanto en procedimientos, orientaciones y actores que intervienen en líneas de prevención y protección.

Desde la protección: normas y orientaciones técnicas sobre procesos de intervención (reparación) con NNA no son adecuadas para el abordaje de violencia sexual en el entorno digital, tampoco existen instrumentos que rijan a programas actuales de intervención (ambulatorios) para identificar vida cotidiana digital de NNA, riesgos y modalidades de victimización sexual[v].

En lo relativo a la detección y denuncia: déficit de herramientas y procedimientos que permitan la identificación oportuna de víctimas y operaciones de rescate, falta de tipificación legal completa de las conductas de violencia sexual digital, brechas presupuestarias para creación y dotación tecnológica suficiente para la detección y persecución de violencia sexual digital, para unidades especializadas de Policías y Ministerio Público. A su turno, las normas investigativas actuales, no se ajustan a los avances de las TIC's, existiendo brechas en el uso de medidas intrusivas para la identificación de interacciones y conductas abusivas sexuales sostenidas en plataformas digitales. Así mismo, existe una baja penalidad en delitos de producción, comercialización y almacenamiento de material abuso de niños, niñas y adolescentes y ausencia de estrategias de detección de potenciales agresores.

4. *¿Cuáles son los retos que existen en el uso de estas tecnologías, productos o servicios digitales, que inhiben la labor de las fuerzas del orden de todas las jurisdicciones en su trabajo de investigación, detección, retirada de material de abuso sexual infantil en línea y persecución de estos delitos?*

Promover el desarrollo de tecnologías que faciliten la identificación de víctimas de violencia sexual en entornos digitales y el diseño, implementación, uso y gestión de la inteligencia artificial (en adelante IA) para mitigación de riesgos, como se verá más adelante. Así mismo, la protección de la privacidad de comunicaciones en dichos entornos y la adopción de medidas legislativas y reglamentarias que promuevan un uso (no nocivo) de tecnologías como la IA en investigaciones, que faciliten la detección y persecución.

Se presenta como reto, la especialización de los actores del sistema penal, pues existe una cultura de ilicitud física, que aminora la gravedad de violencia sexual consumada en entornos digitales, lo que puede impactar en los esfuerzos investigativos para la identificación de agresores en delitos de producción y/o abusos digitales[vi], acotándose las investigaciones y condenas en el almacenaje de dicho material.

Finalmente, el domicilio de agresores se identifica como reto a mejorar en materia de competencias jurisdiccionales para la identificación de agresores, y para ello se debe reforzar la coordinación oportuna y eficaz entre las fuerzas de orden y seguridad de diversos países. Por su parte, la ausencia de canales accesibles de denuncia y promoción de estos impide pesquisar violencias sexuales digitales oportunamente, limitándose hoy a la recepción de reportes por parte del ICSE de INTERPOL o las alertas de CYBERTIPLINE (NCMEC), que no resultan ser suficientes. Se torna indispensable promover reportes y denuncias de actividades sospechosas, patrones de usuario e interacciones inapropiadas con NNA.

5. *¿Qué medidas técnicas y reglamentarias pueden adoptar los Estados, la industria tecnológica y los proveedores de servicios en línea (legislativas, reglamentarias, administrativas, institucionales y de otro tipo) para mitigar los riesgos para los derechos humanos asociados a la explotación y el abuso sexuales de los niños en línea, y garantizar una armonización mínima en todas las jurisdicciones jurídicas?*

Como medidas técnicas se identifica el uso de la IA como mecanismo efectivo de mitigación, entre ellas: detección de contenido inapropiado, que facilita medidas de eliminación automática, análisis de comportamientos sospechosos, identificación de patrones sospechosos, uso de IA en verificación de edad de usuarios, filtrado automático de contenidos sospechosos, asistencia y orientación de víctimas, análisis de datos cuantitativos y cualitativos etc. No obstante, esto presenta retos normativos y reglamentarios, en cuanto a la mitigación de riesgos asociados al uso nocivo de la IA.

Otras medidas técnicas son: controles parentales efectivos, educación y alfabetización digital, promover una cultura de actualización de dispositivos y sistemas operativos, seguridad de la información, canales de denuncia claros y accesibles.

Entre las medidas reglamentarias: leyes de regulación integral, centradas en niñez sobre entornos digitales, sistemas y usos de inteligencia artificial y protección de datos personales, normas mínimas de seguridad en internet con foco en prevención y protección. A nivel institucional, la creación de instituciones públicas con facultades y especialización suficiente para control y fiscalización de dichas medidas, y la creación de consejos expertos asesores que promuevan especialización y alianzas pública-privadas.

6. *¿Existen otros ejemplos prácticos de procesos internos de supervisión, denuncia y notificación; establecimiento de organismos reguladores e intervenciones; vías de reparación; procedimientos sólidos de salvaguardia; diligencia debida y evaluación de riesgos en materia de derechos del niño; y procesos de establecimiento de normas técnicas para garantizar la seguridad y la inclusión desde el diseño?*

Si bien en Chile no se identifican, se debe destacar la labor del National Missing and Exploited Center (NCMEC) en el diseño, gestión e implementación del sistema de Cybertipline y su relación con la Oficina de Programas de Justicia del Departamento de Justicia de Estados Unidos, la que le asignó la tarea de administrar el programa de distribución secundario de alertas AMBER.

7. *En el caso de la Inteligencia Artificial generativa y el cifrado de extremo a extremo, ¿cuáles son los retos y las medidas de mitigación recomendadas, incluida la aplicación de la tecnología avanzada que necesitan las empresas tecnológicas, los proveedores de servicios en línea y las fuerzas y cuerpos de seguridad para prevenir mediante el bloqueo el intercambio y la eliminación de CSAM?*

Como medidas de mitigación del uso nocivo de la IA generativa se sugieren: 1) fomentar la transparencia y responsabilidad en el diseño y uso de IA (considerando el reforzamiento de estándares sobre responsabilidad social empresarial a nivel legal, reglamentario y ético); 2) fomentar inversión en profesionales altamente cualificados que puedan diseñar, implementar y gestionar sistemas de IA en especial en modelos de generación de imágenes[vii] con barreras sobre creación de contenido abusivo; 3) y como ya se ha relevado, la propia IA puede colaborar a crear medidas de mitigación tales como detección y bloqueo de contenido inapropiado, siendo indispensable focalizar desarrollo de tecnología como barreras para "Prompts"[viii].

En cuanto al cifrado de extremo a extremo, el reto es la eventual colisión con los derechos de privacidad y protección de datos personales. No obstante, es necesario abrir un debate técnico al respecto, ya que dicho cifrado imposibilita labores de detección y de persecución de violencias sexuales digitales.

8. *¿Existen ejemplos de medidas proactivas adoptadas para facilitar la consulta y la participación de un amplio abanico de partes interesadas, incluidos los niños y las organizaciones de defensa de los derechos del niño, con el fin de informar la política y la legislación, establecer normas técnicas y aplicar procesos para erradicar el abuso y la explotación sexual infantil en el entorno digital?*

Se destaca: Proyecto Disrupting Harm[ix], la estrategia global de la UE sobre los Derechos del niño[x], los programas implementados por socios estratégicos de la UIT[xi] tales como Programa Ciber paz Egipto y el Programa Europeo de Internet Segura, todos los cuales promueven una participación del sector público, privado y de niños, niñas y adolescentes como *stakeholders* de principal prioridad e interés.

Los ejemplos nacionales son escasos, no obstante, destacan estudios realizados por organizaciones civiles colaborando con el mundo académico que han favorecido recoger experiencias de dichos grupos de interés, en materia de entornos digitales[xii].

9. *¿Qué mecanismo podría establecerse para apoyar y coordinar la participación internacional de la industria pública y privada sobre las amenazas existentes y emergentes de las tecnologías digitales para los niños, para garantizar la armonización y la integración de los esfuerzos nacionales y regionales en la lucha contra este fenómeno?*

Crear Alianzas Público-Privadas sobre desarrollo y usos seguros y responsables de las TiC's y entornos digitales, que sirva de hoja ruta tanto para la creación e implementación de legislación, políticas públicas, desarrollo de tecnologías en aras de protección digital, con mínimos transversales, promoviendo acuerdos y lineamientos estratégicos entre el sector público y empresarial en la región.

RECOMENDACIONES

1. Promover el diseño, creación e implementación de políticas públicas en materia de ciberseguridad infantil, entornos digitales y desarrollo de TIC's con enfoque en niñez y adolescencia, con participación en su diseño de todos los *stakeholders* relevantes, en especial niños, niñas y adolescentes.

2. Promover legislación domestica que regule entornos digitales, ciberseguridad infantil e inteligencia artificial, sustentando normativamente una responsabilidad legal de personas jurídicas en tales modelos de negocio, y creación de institucionalidad pública robusta y especializada con facultades suficientes de control y fiscalización

3. Promover Alianzas Público-Privadas sobre desarrollo y usos seguros y responsables de TIC's y la creación de Consejos asesores expertos.

4. Promover la Responsabilidad Social Empresarial y gobernanzas de sostenibilidad (ESG) en la industria tecnológica y en proveedores de servicios, conforme a estándares dados por OCDE y ONU.

5. Promover la investigación científica para la creación de tecnologías de mitigación de riesgos en entornos digitales y de inteligencia artificial, fomentando el uso de la IA en modelos de ciberseguridad, pero enfatizando controles asociados al diseño y uso de modelos de IA como la generativa y sus usos perjudiciales.

REFERENCIAS

[i] Conforme a datos disponibles en el Observatorio de Derechos de la Defensoría de la Niñez correlacionado con datos de la Subsecretaría de Prevención del Delito, durante el año 2022 la mayor tasa de delitos asociados a material abusivo en entornos digitales fue el de almacenamiento de dicho material. Disponible en: https://observatorio.defensorianinez.cl/

[ii] Pontificia Universidad Católica de Valparaíso (2023), Sistematización de experiencias de abordaje y propuesta de un modelo de intervención de la explotación sexual comercial de niñas, niños y adolescentes en entornos digitales. 14. Disponible en: https://plandeaccioninfancia.ministeriodesarrollosocial.gob.cl/storage/cms/document/nqPWEAehVzI2kSt5htwC9GNzY6ZZA7Mmli6aiPHj.pdf

[iii] Véase Radiografía Digital VTR 2024, Disponible en: https://vtr.com/radiografia-digital

[iv] Nota explicativa: Si bien se reconocen avances legislativos como la promulgación de la Ley N° 21.663 Ley Marco de Ciberseguridad, que crea la Agencia Nacional de Ciberseguridad, su normativa no alcanza a al sector privado ni a servicios no calificados como esenciales, sin perjuicio además de que su vigencia se encuentra supeditada a la potestad reglamentaria del Presidente de la República.

[v] Pontificia Universidad Católica de Valparaíso (2023), p. 18.

[vi] Véase presentación de PDI Jefatura Nacional de Cibercrimen, ante Comisión de Familia, Cámara de Diputados y Diputadas, 06 de mayo de 2024, la cual se adjunta como anexo.

[vii] Nota explicativa: Conforme a recomendaciones realizadas por la Comisión Europea.

[viii] Nota explicativa: se utiliza el concepto Prompts, para referirse a la solicitud o instrucción dada a la IA para que realice una tarea o proporcione información.

[ix] Disponible en: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Proyecto-Disrupting-Harm

[x] Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0142

[xi] Unión Internacional de Comunicaciones, disponible en: https://www.itu.int/itunews/manager/display.asp?lang=es&year=2009&issue=04&ipage=06&ext=html

[xii] Disponible en: https://plandeaccioninfancia.ministeriodesarrollosocial.gob.cl/storage/cms/document/nqPWEAehVzI2kSt5htwC9GNzY6ZZA7Mmli6aiPHj.pdf