**Comentarios de Al Sur al *Draft General Comment No. 25 (202x): Children’s rights in relation to the digital environment*.**

Autor: miembros de Al Sur

Fecha: 14 de noviembre del 2020

1. **Introducción**

Al Sur[[1]](#footnote-1) es un consorcio de organizaciones que operan en la sociedad civil y la academia en ocho países de América Latina, trabajando juntos para fortalecer los derechos humanos en el entorno digital de la región.

Nuestros miembros son:[[2]](#footnote-2) ADC (Argentina), CELE (Argentina), Coding Rights (Brasil), Derechos Digitales (Latinoamérica), Hiperderecho (Perú), IDEC (Brasil), InternetLab (Brasil), IPANDETEC (Panamá), Karisma (Colombia), R3D (México) y TEDIC (Paraguay).

Los miembros de Al Sur han colaborado en esta contribución sobre los derechos de niños, niñas y adolescentes (NNA) en el contexto digital, incorporando evidencia regional y diversas experiencias en el debate de políticas en América Latina. En las siguientes páginas, indicamos secciones del borrador original donde desarrollamos comentarios generales y específicos a cada párrafo.

1. **Comentarios**
* ***Introduction***

En un comentario general, sugerimos reconocer explícitamente dos barreras que enfrentan las niñas y adolescentes en relación con sus derechos en el contexto digital, y que se pueden incorporar tanto en la Introducción del documento como en la sección: "A. El derecho a la no discriminación (art. . 2) "y" G. Difusión de información, sensibilización y formación ".

1. Roles de género estereotipados que, muchas veces, impiden que las niñas y adolescentes accedan y se apropien de tecnologías. La documentación reciente de la ONU así también lo ha establecido. Por ejemplo, el informe reciente de la Unión Internacional de Telecomunicaciones (UIT) titulado "Guidelines for policy-makers on Child Online Protection" (2020), dice:[[3]](#footnote-3)

*"In terms of digital gender divide, research shows that in every region except the United States of America, male Internet users largely outnumber female users. In many countries, girls do not have the same access opportunities as boys, and where they do, girls are not only monitored and restricted in their Internet usage to a much greater extent, but they may also find their safety at risk in efforts to access the Internet" (p.3).*

1. Aunque es nombrada someramente en la sección del draft llamada “Violence against children (arts. 19, 24 (3), 28 (2), 34, 37 (a) and 39; OPSC; OPAC)”, sugerimos posicionar a la violencia de género en las TIC con mayor relevancia a lo largo del texto, ya que muchas evidencias demuestran que son principalmente niñas y adolescente quienes están exponencialmente más a expuestas a la violencia de género, afectando su acceso, apropiación y goce de los derechos del entorno digital. Como ha reconocido la Comisión Interamericana de Derechos Humanos (CIDH)::[[4]](#footnote-4)

*“Debido a la accesibilidad de estas tecnologías para una importante población, la Comisión*

*destaca que las niñas y adolescentes en particular se enfrentan a un riesgo elevado de actos de violencia y discriminación como, entre otros, el acoso, el grooming, las amenazas, el chantaje y el acoso sexual; la carga y/o difusión de fotos íntimas, videos o clips de audio sin su consentimiento; al acceso o divulgación de sus datos privados sin su consentimiento; a la carga y difusión de fotos o videos modificados de niñas y adolescentes como material de pornografía; creación de perfiles falsos, etc.” (p.140-141).*

* ***The best interests of the child (art. 3, para. 1):***

**Párrafo 13**: Considerar toma de decisiones por agentes privados que también deberían de tomar en consideración los mejores intereses de los niños y niñas.

Sugerencia de adición: *States shall ensure that in all decision-making regarding the provision, regulation, design and management of the digital environment that may impact children’s rights, the best interests of the child shall be a primary consideration, including when such decisions involve non-state actors, especially the private sector.*

**Párrafo 14**: En América Latina, un argumento genérico de protección de la infancia es comúnmente utilizado para justificar medidas restrictivas a libre expresión en línea y/o de desproporcionada vigilancia. Considerando la necesidad de garantizar esos derechos, incluso para los niños y niñas, es importante precisar cómo esos derechos deben ser tomados en consideración y la necesidad de equilibrio.

Sugerencia de adición: *The best interests of the child should never be used as an excuse for disproportionate surveillance measures or restrictions to freedom of expression online*.

* ***Right to life, survival and development (art. 6)***

**Párrafo 16**: Es necesario agregar alguna consideración sobre la necesidad de equilibrio y quizás un lenguaje más decisivo contra medidas que impliquen vigilancia masiva. En otras palabras, sugerimos que se especifique que las medidas adoptadas deberían observar las debidas recomendaciones específicas de derechos humanos.

* ***D. The right to be heard (art. 12):***

**Párrafo 19**: Sería bueno especificar que la información recogida de NNA y de víctimas no se usará para monitoreo comercial, se anonimizará adecuadamente, y se revisarán las medidas adoptadas para asegurarse que la tecnología no haya superado las medidas técnicas adoptadas, todo con el objetivo de proteger sus derechos y evitar la revictimización.

* ***Evolving capacities (art. 5)***

**Párrafo 21**: Dudas de interpretación sobre la frase “*the nature of the risks involved in balance with the importance of taking risks in supported environments in order to develop resilience”*.

Es necesario aclarar cómo se logra el justo equilibrio y quién toma y cómo se toma la decisión sobre adecuación (*States should require digital providers to offer or make available services to children appropriate for their evolving capacities*). "Should require" impone la obligación a los proveedores de determinar qué contenidos y servicios son apropiados para los NNA, de acuerdo a la edad de desarrollo en el que están. Esto quizás podría limitar el derecho de acceso a información y educación por parte de los NNA. ¿Qué política, estudio o qué se usará como fundamento para que los Estados determinen lo anterior? ¿Dónde comienza y hasta dónde llega el deber-derecho de los padres para decidir los contenidos para el desarrollo integral y bienestar de su NNA, y dónde comienza la obligación de las plataformas respecto a la disposición o limitación del contenido al que tendrá acceso un NNA? Las legislaciones en materia de familia y derechos de los NNA abordan este tema de manera distinta y es necesaria una visión amplia para no crear contradicciones que hagan inoperantes las normas.

Se sugiere agregar: *As part of their obligations to respect, protect and promote human rights, online service providers should also consider children's evolving capacities in the design of their products or services*.

* ***General measures of implementation by States (art. 4)***

**Párrafo 23**: Falta mencionar al sector privado que también desarrolla políticas. Cuando se trata del ambiente digital, el sector privado tiene un rol relevante en la definición de normas y prácticas y es fundamental que sea expresamente mencionada su responsabilidad en observar la garantía de derechos.

* ***Legislation***

Párrafo 24: Aunque está bien, parece un alcance bastante amplio ordenar evaluaciones de impacto, sin estar definidas en su objetivo y parámetros, para desarrollar legislación. Vale la pena evaluar si es necesario conducir de manera directa a la regulación para esas evaluaciones, sin considerar otras opciones como mejorar las prácticas, educar, etc.

Asimismo, un punto problemático es la propuesta de reformas legislativas para adecuación al ambiente digital: cabe agregar un "*If considered necessary*," al comienzo del párrafo 24.

* **Comprehensive policy and strategy**

**Párrafo 27**: La redacción es aún muy general. ¿Cómo llevarlo a la práctica? ¿Qué debemos entender o qué es una protección efectiva y cómo deben ser las políticas para que sean efectivas? Si este párrafo permanece, se sugiere agregar alguna limitación a regulaciones o vigilancia excesiva en línea con otros estándares de derechos humanos.

* ***Coordination***

**Párrafo 28**: Es muy dudosa la implementación de lo que sugiere este párrafo sin sugerencias de mecanismos. Es también muy ambicioso sugerir un órgano específico para "*coordinate policies and programmes related to children’s rights in the digital environment*". Sugerimos que es mejor sugerir que los sistemas de protección a NNA reciban capacidades necesarias para dar cuenta de los desafíos relacionados al ambiente digital, como prioridad.

* ***Data collection and research***

**Párrafo 31:** Este es un punto muy problemático y donde están ausentes mejores contrapesos. Puede ser usado para justificar la intrusión en los datos y vida privada de NNA.

La primera opción es eliminar el párrafo, en razón de su lenguaje genérico y ambiguo, dado que conlleva riesgos a otros derechos. La segunda opción es proponer que políticas públicas/regulación, etc, deben basarse en participación, estudios y evidencias, y hacerse cargo de cuestiones puntuales:

1. ¿Qué debemos entender por '*data that is adequately resourced*'? Los malos datos tienen consecuencias letales: Gabriel Fernández de EUA[[5]](#footnote-5), sufrió maltrato infantil y murió porque la data que recogían los trabajadores sociales de las instituciones no era fiable, porque recibía maltrato en su casa. ¿Cuán invasivo es "adecuado" siendo todavía efectivo?
2. “*Should inform regulation*”. ¿Qué métodos se usarán para poner a prueba esta data recogida? Se sugiere alguna mención en tal sentido a mecanismos para esa decisión.
3. “*Should be in the public domain*”. Se sugiere agregar algún resguardo explícito sobre anonimización y seguridad. No debería dar lugar a ningún tipo de perfilamiento o interconexión de los datos en el futuro, y que termine afectando los derechos de los NNA.
* ***The business sector***

**Párrafo 37**: El alcance de la redacción es muy amplio, lo que es problemático en línea con lo mencionado anteriormente sobre estimular prácticas de restricción y vigilancia. ¿Prevenir de manera absoluta o adoptar medidas para prevenir? ¿Cómo/quién define "*timely*", "*safety*"?

**Párrafo 39**: Aquí es necesario alinear el lenguaje con los otros documentos existentes en la materia y agregar las referencias adecuadas (Manila Principles, reportes de la relatoría especial de la ONU sobre libertad de expresión de David Kaye, etc.), así como referencias al respeto a los derechos humanos (además de *ethics*, *privacy* and *safety*).

* ***Commercial advertising and market***

Los párrafos permiten el marketing hacia NNA, siempre que sea apropiado a su edad y siempre que no se base en su registro digital, gustos, características, etc. Esto plantea varias incógnitas: quién determina lo que es apropiado o no, cómo se asegura que el marketing no use sus registros digitales. El marketing digital se basa enteramente sobre el perfilamiento y segmentación.

No asumir el daño de la publicidad infantil a los derechos de los NNA, podría ser un retroceso a lo que está presente en reglamentos nacionales incluso. Los ejemplos utilizados en la actual redacción del draft dan a entender que el daño a derechos ocurriría sólo en situaciones extremas cuando, en realidad, puede registrarse incluso en cosas supuestamente bien intencionadas, como sugerencias de libros basado en el registro de actividades.

* ***Access to information (arts. 13 and 17)***

**Párrafo 52:** Es importante reforzar consideraciones sobre pluralismo y diversidad (incluso en términos de quienes son dueños de medios digitales, en considerar fuentes/medios de comunicación públicos, comunitarios y privados). La manera del Estado de proveer esos contenidos incluye la promoción de contenidos desde instituciones públicas (bibliotecas, museos, universidades, medios de comunicación públicos, etc.). Relacionado a ese punto es relevante incluir lenguaje sobre limitaciones de propiedad intelectual como limitaciones al acceso a información por parte de NNA, y recomendar medidas para el acceso al menos de contenidos que cuenten con fondos del Estado.

**Párrafo 55**: Es necesario fortalecer las limitaciones a las restricciones; legitimidad, proporcionalidad, etcétera.

**Párrafo 57**: Es necesario agregar algo sobre el filtrado automático de contenidos. Ahora bien, puede ser problemático que el Estado valide las reglas privadas, no obstante, se sugiere exigir que tales reglas respeten estándares internacionales de DDHH aplicables. Sobre filtros y controles, una vez que existan es probable que sean usados y/o abusados para restringir el acceso a información, expresión y privacidad de los NNA, como ya ocurre. Deben agregarse mecanismos para evaluarlos, modificarlos y retirarlos.

* ***Freedom of thought, conscience and religion (art. 14)***

**Párrafo 64**: Sugerimos tomar un paso más audaz y prohibir cualquier tipo de perfilamiento. En principio, los derechos de NNA son incompatibles con el perfilamiento automatizado para cualquier fin, incluso educativo.

* ***Freedom of association and peaceful assembly (art. 15)***

Como comentario general, considerar hacer mención explícita a vigilancia estatal, considerando que son prácticas que han afectado a jóvenes en América Latina recientemente.[[6]](#footnote-6)

* ***Right to privacy (arts. 16)***

**Párrafo 70**: Se sugiere no asumir intenciones de la recolección de datos. Importante agregar una consideración sobre la relación entre privacidad y otros derechos, haciendo hincapié en la idea del libre desarrollo de la personalidad.

**Párrafo 71**: Originalmente, la frase está escrita así: *Interference with a child’s privacy is only permissible if it is neither arbitrary nor unlawful (article 16)*. Sugerimos una inversión de lenguaje: *"interference ... is not permissible, unless..."*

**Párrafo 72**: Se sugiere no solo hablar de servicios cuando se refiere a la privacidad por diseño, sino también de “*devices, and tools*”. Asimismo, se debería sacar la mención a que eso se limitaría a servicios que impactan a los NNA, pues el estándar debiese ser genérico.

Se sugiere agregar aquí o como párrafo aparte, **la prohibición del uso de sistemas de reconocimiento facial para identificar a los NNA y destacando que los Estados deben eliminar todos los datos personales de los NNA de las bases de datos criminales en línea abiertas al público**.

Esta sugerencia se basa en que las autoridades policiales utilizan cada vez más la tecnología de reconocimiento facial para dirigirse a personas en muchos países del mundo. Esta tendencia es particularmente peligrosa si se usa para identificar a NNA.

Por ejemplo, en abril de 2019 el gobierno de la ciudad de Buenos Aires (Argentina) implementó un sistema de reconocimiento facial conectado a la base de datos pública nacional de personas buscadas por la justicia. La lista contiene 61 niños y, según el relator especial de la ONU sobre el derecho a la privacidad, "sería difícil de justificar como en el interés superior del niño, como lo obliga la Convención de los Derechos del Niño".*[[7]](#footnote-7)(p. 13.4).* Además, la base de datos fue publicada en línea por el Ministerio de Justicia y Derechos Humanos de Argentina y, como resultado, cualquiera podía acceder a los nombres, edades, números de identificación nacional de los menores sospechosos, el presunto delito y la ubicación y la autoridad que emitió la orden de arresto.[[8]](#footnote-8) Al respecto, el Relator también señaló que "la convención también reconoce el derecho de todo niño acusado de haber infringido la ley penal" a que se respete plenamente su privacidad en todas las etapas del proceso "(artículo 40.b.2.vii ), lo que sería incompatible con la publicidad de las órdenes de detención contra menores"[[9]](#footnote-9)*(p.13.4).*

**Párrafo 76:** Se sugiere inversión de lenguaje para recalcar el carácter excepcional de la vigilancia. Si no, se aleja o contradice un poco con el párrafo 77.

**Párrafo 77**: Se sugiere agregar prohibición a obligar el uso de ciertas plataformas que recolectan datos en contextos educacionales u otros.

**Párrafo 78**: Considerar expresamente el uso de seudónimos también. Considerar protección de la identidad de NNA involucrados en acciones/disputas judiciales, condenados o acusados de delitos en los medios digitales.

* ***Birth registration and right to identity (arts. 7 and 8)***

El uso de sistemas digitales de registro de nacimientos podría ayudar a prevenir casos de violaciones de los derechos de los NNA. Sin embargo, se deben tener en cuenta algunas cuestiones al implementar estas tecnologías. Así como es posible que la integración del registro de nacimiento con los sistemas de identidad digital facilite el acceso de los NNA a los servicios, también puede impedirlos si estos registros se constituyen como condición de acceso y ejercicio de derechos. Si el registro es una condición de acceso a los servicios públicos, como la salud pública y la educación, afectaría principalmente a los NNA que dependen de estas políticas para su pleno desarrollo.

En muchos estados (Brasil y Ghana, por ejemplo, han estado implementando certificados de nacimiento biométricos), el registro de nacimiento digital está asociado con la recolección de datos biométricos. Existen algunos riesgos con respecto a las tecnologías biométricas, ya que los datos biométricos son datos sensibles, que deben tener protocolos de tratamiento específicos. Los datos biométricos son un dato único y permanente, y si se replican y almacenan, el interesado ya no es el "único poseedor de sus propios datos biométricos" (UNICEF, 2019).[[10]](#footnote-10) Por lo tanto, este tipo de tecnología debe guiarse por el principio de limitación de propósito, minimización de datos y privacidad infantil. Al abordar el uso del registro de nacimiento digital, es necesario tener en cuenta también a aquellos países que han adoptado el registro biométrico, ya que es una tecnología mucho más invasiva para los datos y la privacidad de los NNA.

Los Estados que implementan los registros digitales de nacimiento y los registros biométricos de nacimiento deben tener protocolos estrictos sobre seguridad e intercambio de datos, además de protocolos de transparencia. Estos datos, si se accede indebidamente, pueden incluso facilitar las prácticas que pretende evitar. Por eso es fundamental que exista una protección adecuada.

Así, nuestra sugerencia **es retirar la promoción de sistemas digitales mientras no se diseñe integralmente una mejor gestión de la identidad**, y listar los ejemplos como "*could*" en vez de "*should*", además de exigir evaluaciones de impacto y auditorías.

* ***Violence against children (arts. 19, 24 (3), 28 (2), 34, 37 (a) and 39; OPSC; OPAC)***

Como sugerimos anteriormente, existe evidencia de organismos regionales con respecto a la violencia de género que afecta a niñas y adolescentes a lo largo de su experiencia en línea. Podría ser relevante agregar una mención especial a eso, ya que la prevención y los remedios deben tener un enfoque de género para ser significativos.

El género debe tomarse desde un punto de vista interseccional. Según el informe “¿Libertad en línea?, Elaborado por Plan International”[[11]](#footnote-11), el 77% de las niñas en Brasil sufrieron acoso en línea. El número es significativamente más alto que el que se encontró en otras partes del mundo (58%). Entre las violencias identificadas por el informe se encuentran amenaza de violencia sexual, acoso sexual, comentarios racistas y / o LGBTQIA +, persecución, lenguaje abusivo, etc. En el escenario de la pandemia, en el que los NNA están cada vez más conectados, también son más vulnerables a este tipo de violencia.

En este contexto, la educación sexual y de género, adaptada a la edad de los niños, niñas y adolescentes, es fundamental para prevenir violaciones de sus derechos básicos. Es fundamental educar a los niños, niñas y adolescentes sobre sus derechos sexuales y reproductivos y enseñarles a ellos, a sus familias y educadores, cómo identificar y prevenir situaciones de abuso y explotación.[[12]](#footnote-12)

**Párrafo 85**: Alentamos a no confundir el "sexting" como una práctica sexual relacionada con el abuso infantil. El sexteo se define como "el envío o la recepción de palabras, imágenes o videos sexuales a través de la tecnología, generalmente un teléfono móvil".[[13]](#footnote-13) El sexteo es una práctica sexual común y no está relacionado con compartir imágenes sexualizadas de NNA, necesariamente. Mezclar estos conceptos podría dañar las formas legítimas de expresión sexual en Internet y conducir a la criminalización del sexteo.

* ***Children with disabilities (art. 23)***

Solamente menciona medidas universales de acceso y diseño, pero no menciona facilidades o flexibilizar los derechos de propiedad intelectual para adaptar contenidos. Se sugiere agregarlo como párrafo separado. Agregar consideraciones sobre accesibilidad y estandarización en la web como obligaciones del Estado, además de las tecnologías de asistencia.

* ***The right to education (arts. 28, 29)***

**Párrafo 109:** Incorporar mención a flexibilización de protección de derechos de autor para fines educativos explícitamente aquí.

* ***Protection from economic, sexual and other forms of exploitation (arts. 32, 34, 35 and 36)***

**Párrafo 121**: Excluir del párrafo la frase '*including hacking*' para evitar la asociación del hackeo a crímenes graves. Si es necesario, especificar "ciberdelitos" y "robo de información privada" o algo similar.

\*\*\*\*\*

1. https://www.alsur.lat/ [↑](#footnote-ref-1)
2. https://www.alsur.lat/quienes-somos [↑](#footnote-ref-2)
3. https://www.itu.int/dms\_pub/itu-s/opb/gen/S-GEN-COP.POL\_MAKERS-2020-PDF-E.pdf [↑](#footnote-ref-3)
4. IACHR. 2019. "Violence and Discrimination Against Women and Girls in Latin America and the Caribbean" http://www.oas.org/es/cidh/informes/pdfs/ViolenciaMujeresNNA.pdf [↑](#footnote-ref-4)
5. https://www.bbc.com/mundo/noticias-51713493 [↑](#footnote-ref-5)
6. https://www.oas.org/es/cidh/prensa/comunicados/2020/018.asp [↑](#footnote-ref-6)
7. UN, 2019 "Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019" https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E [↑](#footnote-ref-7)
8. Human Rights Watch, 2020 "Argentina: Child Suspects’ Private Data Published Online" https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online [↑](#footnote-ref-8)
9. See footnote 4 [↑](#footnote-ref-9)
10. UNICEF. Faces, fingerprints and feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs. UNICEF: 2019. [↑](#footnote-ref-10)
11. PLAN INTERNATIONAL. Liberdade on-line? Como meninas e jovens mulheres lidam com o assédio nas redes sociais?. 2020. Available at: https://cdn.plan.org.br/wp-content/uploads/2020/10/LIBERDADE-ON-LINE-20201002-1.pdf [↑](#footnote-ref-11)
12. UNICEF. Relatório Anual da UNICEF Brasil. PORTES, Larissa; COSTA, Paula, 15, n. 42, Feb., 2019. [↑](#footnote-ref-12)
13. https://www.britannica.com/topic/sexting [↑](#footnote-ref-13)