5RIGHTS FOUNDATION

Hacia entornos digitales seguros en Uruguay

Contribución a la consulta pública sobre niñez y adolescencia, entornos digitales e inteligencia artificial

En Uruguay, las tecnologías digitales influyen en casi todos los aspectos de la vida y el desarrollo de las niñas, niños y adolescentes, desde la forma en que aprenden y juegan hasta cómo se expresan. El último estudio Kids Online Uruguay reveló que nueve de cada diez niñas, niños y adolescentes escolarizados encuestados accedían a Internet a diario desde su casa, y siete de cada diez lo hacían a diario desde su centro educativo.(1)

Sin embargo, los productos y servicios digitales de los que la niñez y adolescencia dependen para su educación, atención médica, entretenimiento, participación cívica y relaciones suelen estar diseñados para priorizar las ganancias comerciales a costa de ellos, exponiéndolos a riesgos incorporados deliberadamente.(2)

Ante una explotación comercial sin precedentes, celebramos que Uruguay preste atención al impacto que las tecnologías digitales tienen en la vida de las niñas, niños y adolescentes. Esto representa una oportunidad crucial para establecer normas mínimas que garanticen una innovación respetuosa de los derechos y para exigir a las empresas tecnológicas que respeten los derechos y el interés superior de la niñez tanto en el diseño como por defecto, de modo que las niñas, niños y adolescentes de Uruguay puedan disfrutar de los beneficios de la tecnología sin verse sometidos a la vigilancia ni a la manipulación comercial.

Riesgoso por diseño

Si bien las tecnologías digitales ofrecen oportunidades transformadoras para la niñez, las empresas tecnológicas también la exponen a riesgos significativos que van mucho más allá de contenidos dañinos aislados o de actores malintencionados individuales.

Las empresas tecnológicas fallan sistemáticamente al diseñar productos y servicios digitales pensando en las infancias y, por el contrario, sus modelos de negocio y sus decisiones de diseño priorizan los intereses comerciales por encima de los derechos, la seguridad y el bienestar de la niñez.

Una investigación de 5Rights en México reveló que los perfiles registrados a nombre de niños fueron expuestos, en cuestión de minutos, a contenido relacionado con la autolesión, imágenes sexualizadas y violencia gráfica, incluyendo ejecuciones de cárteles y escenas de reclutamiento.(3) De manera similar, una investigación sobre la IA generativa en Brasil mostró que a la niñez se le promociona contenido sexualizado o inapropiado para su edad, y que se siente resignada ante la extracción constante de datos, la cual se percibe como inevitable. (4)

Los riesgos a los que se enfrentan las niñas, niños y adolescentes están presentes en todo el mundo digital, desde las redes sociales y los videojuegos hasta la tecnología

educativa, los dispositivos conectados y los sistemas de inteligencia artificial (IA), y no son accidentales.

Por el contrario, son el resultado predecible de modelos de negocio y decisiones de diseño optimizados para obtener ganancias comerciales: sistemas de recomendación que promueven la participación, configuraciones predeterminadas que maximizan la extracción de datos y el gasto sin obstáculos, interfaces que recompensan el uso prolongado y funciones que facilitan el contacto potencialmente peligroso con extraños. Hoy en día, el 99% de los sitios web y las aplicaciones utilizan funciones manipuladoras, como el desplazamiento infinito, la reproducción automática y las notificaciones constantes, para maximizar la participación al aprovechar las vulnerabilidades del desarrollo de niñez.(5)

Por lo tanto, centrarse únicamente en la moderación de contenidos pasa por alto las principales causas del daño. Un enfoque sistémico debe examinar cómo las decisiones de diseño dan forma a las experiencias digitales de la niñez, y los productos y servicios deben evaluarse respecto a los impactos de sus modelos de negocio, algoritmos, funciones y configuraciones predeterminadas. Cuando se identifiquen riesgos, se debe exigir a las empresas que modifiquen los sistemas que los generan, en lugar de limitarse a eliminar elementos individuales después de que se haya reportado el daño.(6)

Privacidad y protección de datos

Desde el momento en que un niño o niña abre una aplicación, juega un juego o visita un sitio web, se recopilan, utilizan y almacenan datos personales y se realizan inferencias a partir de ellos. La elaboración de perfiles y la segmentación comercial determinan lo que la niñez ve y con quiénes interactúan, lo que repercute en sus vidas en el mundo físico. Por tanto, la privacidad no es una cuestión ajena a la seguridad en línea, ya que las prácticas abusivas de tratamiento de datos y los diseños riesgosos se refuerzan mutuamente.

Las empresas tecnológicas han condicionado la participación de niñas, niños y adolescentes en el mundo digital a que se sometan a prácticas invasivas diseñadas intencionalmente para recopilar, compartir y vender sus datos con fines de lucro, elaborar perfiles y predecir su comportamiento. Como resultado, autoridades reguladoras a lo largo de los cinco continentes constataron que hoy la niñez enfrenta riesgos para su privacidad más generalizados en el mundo digital que en 2015.(7) Sin embargo, el valor de sus datos y el verdadero alcance de esta explotación comercial siguen siendo, en gran medida, invisibles.

Uruguay cuenta con un importante punto de partida en la Ley 18.331 de Protección de Datos Personales. Su artículo 12, tras su modificación, señala expresamente la responsabilidad proactiva, la privacidad desde el diseño y por defecto y las evaluaciones de impacto en la protección de datos. Estos requisitos proporcionan una base normativa consolidada sobre la cual podrían desarrollarse protecciones específicas para niñas, niños y adolescentes. Sin embargo, no deben considerarse un sustituto de las obligaciones destinadas a abordar la extracción innecesaria de sus datos, incluso cuando no exista un tratamiento ilícito de datos personales.(8)

En particular, el Comité de los Derechos del Niño de las Naciones Unidas llama a establecer salvaguardias de privacidad desde el diseño y prohibiciones legales de elaboración de perfiles o la segmentación de niñas, niños y adolescentes con fines

comerciales a partir de características reales o inferidas. Uruguay puede hacer efectivos estos estándares mediante configuraciones predeterminadas que garanticen un alto nivel de privacidad, minimización de datos, restricciones al intercambio y la conservación de datos, y prohibiciones claras de la explotación comercial de los perfiles de las niñas, niños y adolescentes.(9)

Inteligencia Artificial

Mientras los sistemas de IA pueden presentar oportunidades reales para la niñez, suelen desplegarse a una gran escala antes de que la seguridad y eficacia se hayan demostrado adecuadamente, lo que permite que los incentivos comerciales avancen más rápido que los mecanismos de rendición de cuentas. Al igual que las tecnologías anteriores, los sistemas de IA amplifican los riesgos en el entorno digital: los sistemas de recomendación promueven contenidos y contactos dañinos, los sistemas de IA generativa pueden producir contenidos engañosos o inapropiados; y los sistemas conversacionales pueden manipular a la niñez para involucrarla en interacciones que le resulten difíciles de interpretar o cuestionar.(10)

El Código de Diseño sobre Infancia e IA de 5Rights ofrece una vía práctica para traducir los derechos de las niñas, niños y adolescentes en decisiones a lo largo de todo el ciclo de vida de la IA. Exhorta a quienes diseñan y despliegan sistemas de IA a identificar los riesgos previsibles, realizar pruebas y mitigarlos, garantizar mecanismos claros de rendición de cuentas y proporcionar salvaguardias y vías de reparación. Para Uruguay, esto implica integrar la IA en las obligaciones generales de protección de los derechos de la niñez y exigir un escrutinio adicional cuando determinadas plataformas o servicios de la IA presenten riesgos elevados.(11)

La evaluación de un sistema de IA debe examinar su finalidad prevista, los datos utilizados para su entrenamiento y evaluación, los usos indebidos previsibles, la capacidad de la niñez para reconocer o cuestionar los resultados automatizados y cómo funcionará el sistema una vez desplegado en la práctica. Esta evaluación es especialmente importante cuando se introduce una herramienta de IA en una escuela, un servicio de salud u otro entorno en el que niñas, niños y adolescentes puedan razonablemente considerar que sus recomendaciones tienen autoridad. La obligación debe ser anticipar y mitigar los daños, y no esperar que reconozcan por sí mismos cada limitación técnica.

Por qué las soluciones parciales no son suficientes

La alfabetización digital, el apoyo a las familias, las herramientas de denuncia y una moderación adecuada de contenidos contribuyen a proteger a la niñez en el entorno digital, pero ninguna de estas medidas debe presentarse como una alternativa al diseño de productos y servicios seguros. No se puede esperar que niñas, niños y adolescentes contrarresten por sí mismos los efectos de sistemas perfeccionados para maximizar su interacción, y las configuraciones de control parental no pueden corregir riesgos incorporados deliberadamente en un servicio o producto que podían preverse. La regulación debe atribuir la responsabilidad a las empresas que tienen la capacidad de modificar dichos sistemas.(12)

Por lo tanto, la educación y el apoyo a las familias son complementarios a las políticas públicas, no una evidencia de que las empresas hayan cumplido con sus

responsabilidades. Deben fortalecer la capacidad de niñas, niños y adolescentes para ejercer sus derechos en un entorno que ya esté diseñado para ser seguro. El mismo principio se aplica a la moderación y a las denuncias: responder con rapidez a los incidentes es valioso, pero no exime a un proveedor de su deber de evitar que el diseño de sus productos y servicios exponga a la niñez a daños previsibles.

Del mismo modo, divulgar las prácticas de los sistemas de recomendación, ofrecer términos y condiciones más claros y dar mayor visibilidad a los controles de usuario son medidas valiosas, pero insuficientes si no se acompañan de normas de cumplimiento exigibles, supervisión independiente y vías de reparación efectivas. La transparencia debe garantizar que las empresas rindan cuentas por su conducta, sin trasladar a la niñez la carga de garantizar su propia seguridad.

En ocasiones, puede ser necesario restringir el acceso a funciones de alto riesgo, pero las exclusiones generales basadas únicamente en la edad no corrigen por sí solas los servicios inseguros y pueden interferir con los derechos a la participación, a la información y a la privacidad. Todo requisito de aseguramiento de la edad debe ser demostrablemente necesario, proporcional a un riesgo específico, respetuoso con la privacidad y evaluado de manera independiente, y, además, debe comprobar que una persona usuaria cumple con un umbral de edad sin requerir la determinación de su identidad.(13)

El camino a seguir: los derechos de las niñas, niños y adolescentes en el entorno digital

Hace cinco años, la adopción de la Observación General No. 25 del Comité de los Derechos del Niño de las Naciones Unidas aclaró cómo se aplica, en el mundo digital, la obligación existente de los Estados de proteger los derechos de las niñas, niños y adolescentes. En particular, establece que el interés superior del niño debe ser una consideración primordial en el diseño y la regulación del entorno digital; que los Estados deben exigir procesos de debida diligencia y evaluaciones de impacto sobre los derechos de la niñez; y que las empresas tecnológicas exponen a la niñez a riesgos mediante el diseño y el funcionamiento de sus servicios.(14)

Desde entonces, en todos los continentes han surgido buenas prácticas que consagran estándares de diseño apropiado a la edad y exigen a las empresas tecnológicas que rindan cuentas por el respeto de los derechos de la niñez desde el diseño y por defecto.(15) Cuando la regulación, como el ECA Digital de Brasil o el Código de Diseño Apropiado a la edad del Reino Unido, exige a las empresas tecnológicas demostrar que respetan la privacidad y la seguridad de niñas, niños y adolescentes antes de lanzar sus productos y servicios al mercado, la evidencia muestra que estas refuerzan las protecciones de privacidad en las configuraciones predeterminadas, rediseñan los sistemas de recomendación y restringen la publicidad dirigida a la niñez.(16) Por el contrario, en la ausencia de regulaciones sólidas y de mecanismos efectivos para hacerlas cumplir, las empresas tecnológicas siguen trasladando la responsabilidad a las personas usuarias y ofreciendo salvaguardias desiguales entre jurisdicciones, incluido Uruguay.(17)

5Rights alienta a Uruguay a avanzar hacia una regulación de cumplimiento exigible, basada en derechos, que obligue a las empresas tecnológicas a rendir cuentas mediante un enfoque sustentado en los derechos de la niñez y los derechos humanos. **En palabras simples: se debe exigir a las empresas tecnológicas que demuestren que los**

productos y servicios digitales que puedan afectar a las niñas, niños y adolescentes son seguros y respetuosos de sus derechos antes de su lanzamiento al mercado.

Para cumplir con las obligaciones establecidas en la Convención sobre los Derechos del Niño, instamos a Uruguay a adoptar y hacer cumplir las siguientes medidas interrelacionadas en su futura labor legislativa y regulatoria:

Instamos a los Estados de la región a:

1. **Proteger a todas las niñas, niños y adolescentes en todos los servicios y productos que utilizan.** Definir como niño a toda persona menor de 18 años. Aplicar las protecciones no solo a los productos y servicios comercializados para la niñez, sino a todos aquellos a los que probablemente accedan o que puedan afectarles, incluidos los videojuegos, los servicios de mensajería, los servicios educativos y los sistemas de IA. El ámbito de aplicación debe abarcar a los proveedores que prestan servicios a niñas, niños y adolescentes en Uruguay, independientemente de su domicilio empresarial, con mecanismos adecuados de rendición de cuentas a nivel local. La regulación debe abarcar todos los productos y servicios, no simplemente contenidos individuales.(18)

2. **Exigir evaluaciones de impacto en los derechos de la niñez y medidas de mitigación.** Establecer la obligación de realizar evaluaciones antes del despliegue, cuando se introduzcan cambios sustanciales y, posteriormente, a intervalos regulares. Estas deben considerar a las niñas, niños y adolescentes de distintas edades y circunstancias, abordar los riesgos derivados del diseño y de los modelos de negocio, incluir una participación significativa y dar lugar a medidas de mitigación documentadas. Las evaluaciones deben examinar los efectos combinados de las funcionalidades, no solo su funcionamiento de forma aislada, y actualizarse cuando se disponga de evidencia sobre un riesgo emergente. Las autoridades reguladoras deben estar facultadas para obtener evidencia, exigir auditorías independientes y ordenar el rediseño, la restricción o la eliminación de funcionalidades de alto riesgo.(19)

3. **Establecer estándares de seguridad y privacidad de cumplimiento exigible desde el diseño y por defecto.** Exigir las configuraciones predeterminadas que ofrezcan la mayor protección y prohibir las funcionalidades y prácticas que puedan contribuir a daños conocidos o razonablemente previsibles, incluidos los mecanismos manipulativos destinados a maximizar la interacción y las vías inseguras de recomendación o de contacto. Las obligaciones deben ser tecnológicamente neutrales y considerar los riesgos acumulativos que se generan por las combinaciones de funcionalidades. En los servicios y productos que probablemente utilicen las niñas, niños y adolescentes o que puedan afectarles, la seguridad debe ser una condición de partida, no una configuración que ellos o sus madres y padres deban descubrir y activar.(20)

4. **Prohibir la elaboración de perfiles y la segmentación de niñas, niños y adolescentes con fines comerciales.** Prohibir expresamente la segmentación comercial basada en sus características reales o inferidas, incluida la elaboración de perfiles basados en la pertenencia a grupos o en afinidades. Complementar esta prohibición con restricciones a las prácticas abusivas de recopilación e intercambio de datos, la minimización de datos y configuraciones que garanticen un alto nivel de privacidad desde el inicio. Todo régimen de aplicación y cumplimiento debe distinguir

el tratamiento legítimo y estrictamente necesario de los datos de la creación de perfiles de comportamiento para fines publicitarios y de optimización de la interacción.(21)

5. **Aplicar estas obligaciones durante todo el ciclo de vida de los productos y servicios.** Garantizar que quienes proveen y despliegan sistemas que puedan afectar a la niñez puedan demostrar un diseño apropiado a la edad, pruebas documentadas, una asignación clara de responsabilidades a personas y organizaciones, un monitoreo continuo y vías de reparación accesibles. Abordar los impactos en la privacidad, la equidad, el desarrollo y el bienestar emocional, en lugar de tratar los daños únicamente como una cuestión de moderación de contenidos.(22)

6. **Establecer mecanismos de aseguramiento de la edad focalizados y respetuosos de la privacidad.** Cuando una funcionalidad presente un riesgo específico asociado a la edad, exigir un método de aseguramiento de edad (*age assurance*) adecuado a ese riesgo y no recopilar más información de la necesaria. Proteger el acceso de niñas, niños y adolescentes a servicios beneficiosos y ofrecer vías para impugnar errores. No equiparar la acreditación de la edad con la acreditación de la identidad ni convertir la vigilancia generalizada en el precio de la seguridad. Las obligaciones de seguridad subyacentes deben seguir siendo aplicables incluso cuando asegurar la edad sea técnicamente imperfecto.(23)

7. **Establecer una supervisión efectiva y mecanismos exigibles de rendición de cuentas.** Dotar a las autoridades competentes de las facultades, la capacidad técnica y los recursos necesarios para solicitar evaluaciones de riesgos, verificar el cumplimiento, encargar o exigir auditorías independientes y ordenar medidas correctivas. Las sanciones proporcionales y otras herramientas para hacer cumplir la normativa deben garantizar que el cumplimiento sea algo más que un compromiso voluntario. La coordinación entre los organismos de protección de la niñez, de protección del consumidor y de protección de datos debe evitar vacíos en la supervisión.(24)

8. **Hacer efectivos los derechos mediante vías de reparación y participación.** Exigir términos y condiciones breves, accesibles y apropiados a la edad, explicaciones claras de las decisiones automatizadas y mecanismos confidenciales de denuncia, impugnación y reparación que permitan lograr cambios oportunos. La niñez también debe participar de manera significativa en la elaboración y revisión de las políticas digitales, teniendo debidamente en cuenta la evolución de sus capacidades y sin recopilar sus datos personales de forma intrusiva. Estas medidas fortalecen la rendición de cuentas, pero no sustituyen la prevención de riesgos desde el origen.(25)

La consulta pública de Uruguay ofrece una oportunidad para ir más allá de la respuesta a incidentes individuales en línea y avanzar hacia la prevención de riesgos previsibles desde su origen. Al trasladar los principios de privacidad ya establecidos a obligaciones de cumplimiento exigibles, centradas en los derechos de la niñez y aplicables a toda la gama de productos y servicios digitales, Uruguay puede proteger sus derechos y, al mismo tiempo, garantizar sus oportunidades de aprender, participar y beneficiarse de la tecnología.

Referencias

(1) https://www.unicef.org/uruguay/informes/informe-kids-online-uruguay-2022

(2) https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/ & https://5rightsfoundation.com/resource/pathways-how-digital-design-puts-children-at-risk/

(3) https://5rightsfoundation.com/resource/exploring-what-children-can-see-on-social-media-in-mexico/

(4) https://researchonline.lse.ac.uk/id/eprint/129516/

(5) https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-networks/international-privacy-sweep/2024_sweep/opc-sweep-report-2024/

(6) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/

(7) https://5rightsfoundation.com/children-face-greater-privacy-risks-today-than-a-decade-ago-and-tech-companies-are-to-blame/

(8) https://www.impo.com.uy/bases/leyes/18331-2008/12

(9) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 42 & 70.

(10) https://researchonline.lse.ac.uk/id/eprint/141720 & https://www.ipu.org/resources/publications/issue-briefs/2026-10/protecting-childrens-rights-in-age-ai-parliamentary-action-guide

(11) https://5rightsfoundation.com/resource/children-ai-design-code/.

(12) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 17–28.

(13) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 26–28 and 38–40.

(14) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 12–13 and 35–39

(15) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/.

(16) https://researchonline.lse.ac.uk/id/eprint/123522

(17) https://researchonline.lse.ac.uk/id/eprint/138377/

(18) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 31–34.

(19) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, para. 38 & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 41–43.

(20) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 39 and 96 & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 44–53

(21) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 42 and 70 & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 44–45 and 50–53.

(22) https://5rightsfoundation.com/resource/children-ai-design-code/ & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 46–49.

(23) https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/, pp. 38–40.

(24) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 27 and 35–38 & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/ pp. 58–64.

(25) https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paras. 18, 44 and 70 & https://5rightsfoundation.com/resource/building-a-digital-environment-designed-with-children-in-mind-an-international-best-practices-blueprint/ pp. 54–60.